ID: 680488
Sample Name: SwiftMessage_Unlocked_Transaction ProofMessage.exe
Cookbook: default.jbs
Time: 17:29:13
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

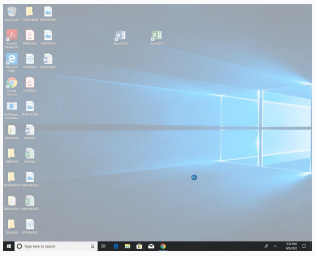
Windows Analysis Report

SwiftMessage_Unlocked_Transaction ProofMessage.exe

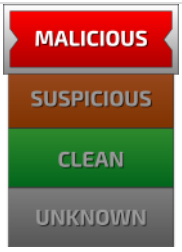
Overview

General Information

Sample Name:	SwiftMessage_Unlocked_Transaction ProofMessage.exe
Analysis ID:	680488
MD5:	ed3e368480ce9f..
SHA1:	d8f888cfee5175c..
SHA256:	3d547c5731a7c0..
Tags:	exe Formbook
Infos:	



Detection



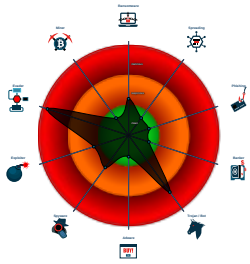
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Queues an APC in another process …
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- SwiftMessage_Unlocked_Transaction ProofMessage.exe (PID: 3144 cmdline: "C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe" MD5: ED3E368480CE9FDD917565B149D52E14)
  - powershell.exe (PID: 4400 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\wKwiksScXFp.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5656 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\wKwiksScXFp" /XML "C:\Users\user\AppData\Local\Temp\tmpFDE9.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SwiftMessage_Unlocked_Transaction ProofMessage.exe (PID: 1888 cmdline: C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe MD5: ED3E368480CE9FDD917565B149D52E14)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 2896 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.familism.net/qaom/"
  ],
  "decoy": [
    "WK4227sGKNxdtoj/0el0mSq6",
    "6xaJ/eBRc1Is34jYrt3HpbWWpL8=",
    "Q7+YyiJbcxwKABQO",
    "atnlwk5WXUDP",
    "O6yJJQ1+qofZlXOe9Tg=",
    "dunCiWrF4HybTdg=",
    "DMu9XSig1sDHpEurphKPD5I=",
    "0BiFGyxxBqHK9SoX",
    "I1T3Eo/xM+g+G8E=",
    "YNCVL0Gu1nybTdg=",
    "LK5/JglqrJNlLXsB/y8=",
    "GVT1r5DUEwmfRB49hQ==",
    "3FgVMp31AavK9SoX",
    "/Go/U5XV/73NRGaYz9Hj",
    "X5wxX+xch3fK9SoX",
    "7zegS4KNMpAEV88=",
    "6h6gMwpSYEpXCpjLqhKPD5I=",
    "gvSwORhos596Mc0rToo1E8p73E0xBu0BkA==",
    "siwQw91WgGlzSOpKMzztMvABuFg1",
    "Z6dAwcEocHDK9SoX",
    "h7Mox9lUflw78oXFrhKPD5I=",
    "xRSnRy6SEr9VuQ==",
    "d/zWB58BGMsb4xZo2gP6",
    "vyfkgl2Xv6k2o+IXStjUFiSiAg==",
    "crBR7fNVZk/nYJClIoVlzw==",
    "HGIDmKrWFPo=",
    "DI1Q7AExpQRXONI=",
    "/388PtNIZxpxZ/cdmFFAxw==",
    "5VYiHn7Y8eF43fj8L9rVFiSiAg==",
    "9UO3sVqQsmLF",
    "sXNmwsknc2xVO/RcUdHKE6fQJZm3zw==",
    "X9SLfeVhiWxQRB49hQ==",
    "j7wwN4PJAqBNr8tn+a4Aeuyt",
    "DE/Zg2Sr23ybTdg=",
    "WsyC+M8HJtukVniYIoVlzw==",
    "/jzqGSaiEr9VuQ==",
    "xSwSx8sWcl+0RB49hQ==",
    "qrSdt0jBEwgbg3sB/y8=",
    "zhiQnTF+5INt3woO",
    "+CK93DWQm0fDrPkh1xKPD5I=",
    "pOBXfOMlTw0Pd7LVml1ibSiz",
    "GItvoylqfzY/K4CiIoVlzw==",
    "/Ww8XPNtlk+qXmRHqaB0mSq6",
    "Uch4GPdKVzshf3sB/y8=",
    "zPNua9dQbiB0Vwpt7Pn4wEoTJBU9",
    "HZtax4/e8dM57w8bojTVvkwTJBU9",
    "uTlOCbAIUnBZUbsO0xKPD5I=",
    "XqUSspnoLSUlBHMQETY=",
    "rSTV4D+7Er9VuQ==",
    "bd3oTDOnF3ybTdg=",
    "pyDqCl2xul22qvLoVuGBZueCJZm3zw==",
    "deyiDdEUUTUaqVezL8S7jZ97lDP8xw==",
    "syQDtrscLQ2kRB49hQ==",
    "KlzKRxhUdxUtj9khEX3IjYLEw+Qb5X0=",
    "l9NbxqQUPC8vBnMQETY=",
    "LaiNxSxCizujRB49hQ==",
    "QLiHqfxYm1kshbv853KG87WWpL8=",
    "kOp/JDkY0qwjrg==",
    "GdW4A7HsB3ybTdg=",
    "QbqiVFmfl0Ma5Slgnh3WHeyBJZm3zw==",
    "DY45YM89dV+1RB49hQ==",
    "aqkyAuctVzMO5X3DqxKPD5I=",
    "WoDzipz+PStyOtgA",
    "lQraDqf9JQnmr/fnLin2qSey"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x65e1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1e160:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8ff:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x172f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x170f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16ba1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x171f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1736f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa4ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x15dbc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb212:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1cdb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1deca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x197f9:$sqlite3step: 68 34 1C 7B E1 • 0x1992c:$sqlite3step: 68 34 1C 7B E1 • 0x1983b:$sqlite3text: 68 38 2A 90 C5 • 0x19983:$sqlite3text: 68 38 2A 90 C5 • 0x19852:$sqlite3blob: 68 53 D8 7F 8C • 0x199a5:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.500415213.00000000005D0000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.SwiftMessage_Unlocked_Transaction ProofMessage.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.SwiftMessage_Unlocked_Transaction ProofMessage.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x57e1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d360:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9aff:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x164f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
8.0.SwiftMessage_Unlocked_Transaction ProofMessage.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x162f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15da1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x163f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1656f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x96ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14fbc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa412:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bfb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d0ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.SwiftMessage_Unlocked_Transaction ProofMessage.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x189f9:$sqlite3step: 68 34 1C 7B E1 • 0x18b2c:$sqlite3step: 68 34 1C 7B E1 • 0x18a3b:$sqlite3text: 68 38 2A 90 C5 • 0x18b83:$sqlite3text: 68 38 2A 90 C5 • 0x18a52:$sqlite3blob: 68 53 D8 7F 8C • 0x18ba5:$sqlite3blob: 68 53 D8 7F 8C
0.2.SwiftMessage_Unlocked_Transaction ProofMessage.exe.4215c38.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 3 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

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

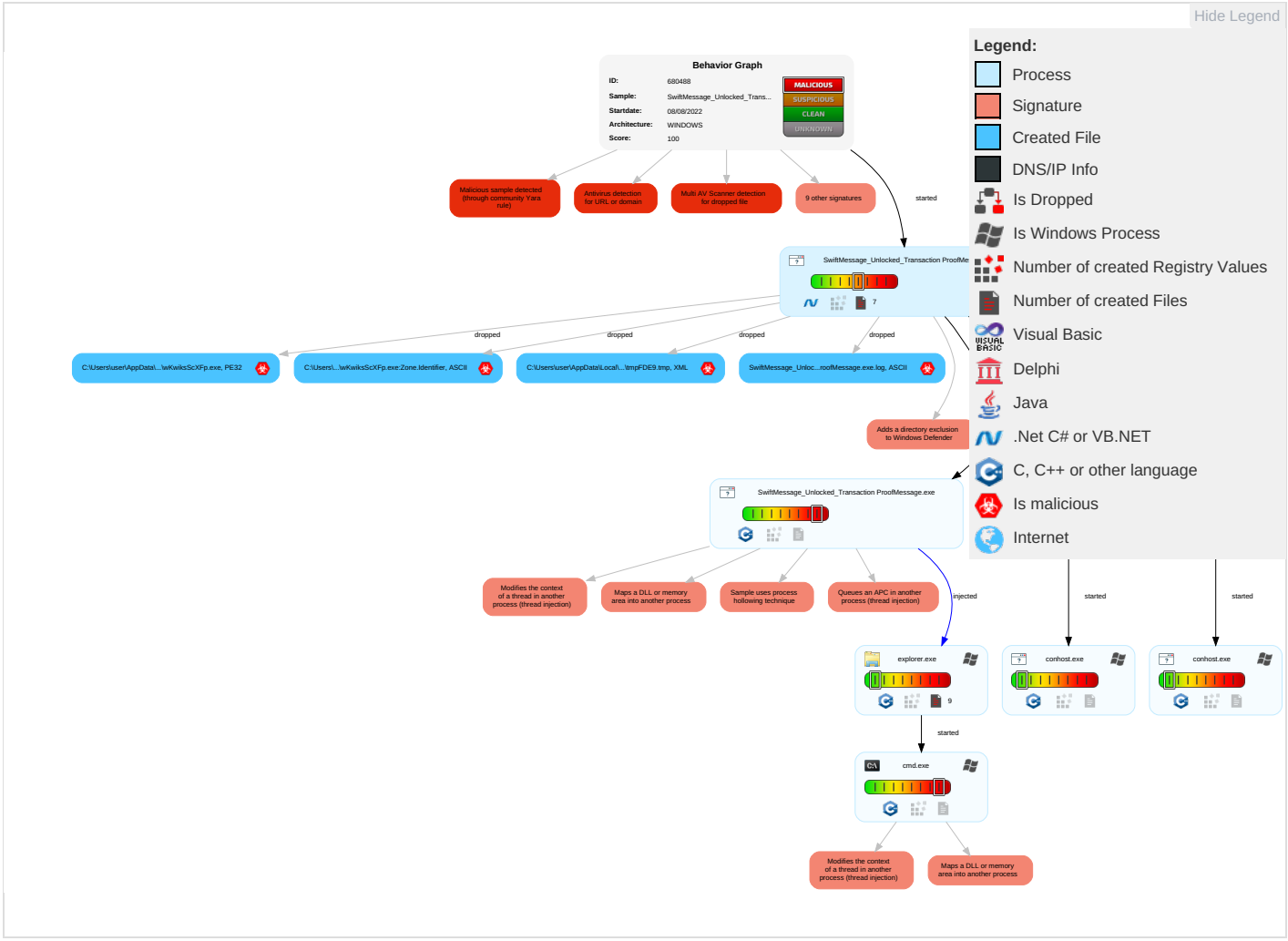
Yara detected FormBook

Yara detected FormBook

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	1 Scheduled Task/Job	1 Scheduled Task/Job	4 1 2 Process Injection	1 Masquerading	1 Input Capture	2 2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 DLL Side-Loading	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information 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	3 Software Packing	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 DLL Side-Loading	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
SwiftMessage_Unlocked_Transaction ProofMessage.exe	38%	Virustotal		Browse
SwiftMessage_Unlocked_Transaction ProofMessage.exe	29%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
SwiftMessage_Unlocked_Transaction ProofMessage.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wKwiksScXFp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wKwiksScXFp.exe	29%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.SwiftMessage_Unlocked_Transaction ProofMessage.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comessedG?1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.familism.net/qaom/	2%	Virustotal		Browse
www.familism.net/qaom/	100%	Avira URL Cloud	malware	
http://www.fontbureau.comd7	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/lnlN?:	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn2	0%	Avira URL Cloud	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comdnF	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb-n	0%	Avira URL Cloud	safe	
http://en.wi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr	0%	URL Reputation	safe	
http://www.carterandcone.comEach4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicTFf	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnZ	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://www.fontbureau.comtoTF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnlg?	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/xN	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comdQ	0%	Avira URL Cloud	safe	
http://www.carterandcone.comz	0%	URL Reputation	safe	
http://www.founder.com.cn/cn6	0%	URL Reputation	safe	
http://www.fontbureau.comltvoN?:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comN?:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalsd7	0%	Avira URL Cloud	safe	
http://www.fontbureau.comE.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.familism.net/qaom/	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designerse1	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241302162.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessedG?1	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241999799.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241648999.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241904236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242364873.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241839678.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242155357.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241815649.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242439729.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242285774.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241677362.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241882852.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242312169.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241936236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242339210.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241860717.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comd7	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242364873.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242155357.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242439729.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242285774.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242312169.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242339210.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242188590.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242263259.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/lnlN?:	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239673589.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238423141.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238640826.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239527886.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239102986.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238618123.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238538445.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239298805.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn2	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237144267.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243054980.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.c	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236573699.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237645977.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237561745.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237725635.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237607822.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237418195.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237253717.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237348551.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237394542.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237371268.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdnF	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241999799.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241648999.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241904236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242364873.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241839678.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242155357.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241622575.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241815649.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242439729.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242285774.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241677362.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241882852.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242312169.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241936236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242339210.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244725982.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244968212.00000000060D8000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245288432.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.249977639.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.247776276.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.246780981.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245690952.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.247331002.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248521016.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.247062279.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248657981.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.246315588.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245384768.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.250073464.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.247030819.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245313604.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245752027.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248203304.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.247267265.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248392812.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.246402353.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersl	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241302162.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/6	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238640826.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239102986.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238618123.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238538445.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnb-n	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wi	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236947938.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238423141.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238640826.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239102986.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238618123.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238538445.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersd	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241339444.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241553390.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241370167.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241401813.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241449552.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnr	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comEach4	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237725635.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comicTFf	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243021518.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242772155.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243338710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242602401.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242880352.00000000060D0000.0000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242632805.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243578782.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243305544.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242810453.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243458235.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243080983.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242746948.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243510605.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243106460.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243054980.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243633570.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243537061.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgrito	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243021518.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242772155.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243338710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242880352.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242632805.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243305544.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242810453.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243458235.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243080983.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242746948.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243510605.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243106460.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243054980.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243537061.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239517946.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239379153.00000000060B2000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comrsiv	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241315732.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241349024.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241370167.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241401813.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241562151.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241449552.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241226152.00000000060D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239298805.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnZ	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237144267.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.285088525.0000000003392000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.281630024.0000000003165000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comtoTF	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243021518.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242772155.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242364873.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242602401.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242880352.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242155357.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242632805.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242810453.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242439729.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242285774.00000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243080983.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242312169.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242552714.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242339210.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242746948.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241648999.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.249977639.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241315732.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243021518.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242772155.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241999799.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241349024.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243338710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248521016.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241648999.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248657981.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.250073464.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241370167.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248392812.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248249433.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244725982.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244841654.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245162197.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245031662.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.245128766.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244923054.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244954693.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244037027.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243761000.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243021518.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242772155.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244069272.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243328710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243727765.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.244008649.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243982106.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242602401.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243789684.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242880352.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243930754.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242632805.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243578782.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243305544.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242810453.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnlg?	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237144267.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comtu	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242395978.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242364873.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242155357.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242439729.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242285774.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242312169.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242339210.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242188590.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242263259.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/xN	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239673589.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239527886.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239102986.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239298805.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239673589.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238423141.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238640826.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239527886.00000000060D5000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238369385.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239298805.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241349024.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241370167.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241622575.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.249977639.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248521016.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248657981.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248392812.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248249433.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comdQ	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241349024.00000000060D4000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241370167.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comz	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.237725635.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn6	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.236463457.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comltvoN?:	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248203304.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248249433.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241999799.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241648999.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242085127.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241904236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00003.242129232.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241839678.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241815649.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242064937.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241677362.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242107807.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241882852.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241936236.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241860717.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.como	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248203304.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.248249433.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000002.300706782.00000000072B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comN?:	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241226152.00000000060D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalic	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.242526099.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/f	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239849647.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240076436.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240030862.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239999372.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239966190.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239773487.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239745515.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239942847.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239102986.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239569461.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239298805.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238795009.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsd7	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243338710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243578782.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243305544.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243458235.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243080983.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243510605.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243106460.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243054980.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243633570.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243537061.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.241188909.00000000060CF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comE.TTF	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243138269.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243170710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243338710.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243282875.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243379848.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243305544.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243458235.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243510605.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243106460.00000000060D0000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.243537061.00000000060D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0-s	SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239159133.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239849647.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240076436.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240030862.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240708870.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238714359.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239999372.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240479501.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239691705.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239966190.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239021418.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240758246.00000000060CF000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239713163.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240663615.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239397382.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240527492.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239773487.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.238640826.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239745515.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.240437508.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, SwiftMessage_Unlocked_Transaction ProofMessage.exe, 00000000.00000003.239942847.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680488

Start date and time: 08/08/202217:29:13	2022-08-08 17:29:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SwiftMessage_Unlocked_Transaction ProofMessage.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 59.9% (good quality ratio 52.3%) • Quality average: 71.9% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 80.67.82.235, 80.67.82.211
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
17:30:25	API Interceptor	2x Sleep call for process: SwiftMessage_Unlocked_Transaction ProofMessage.exe modified
17:30:33	API Interceptor	41x Sleep call for process: powershell.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\SwiftMessage_Unlocked_Transaction ProofMessage.exe.log

Process:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22236
Entropy (8bit):	5.602477475466931
Encrypted:	false
SSDEEP:	384:UjtCD+0jMnIImRR3ISBKnYjsSC7Y9glSJ3x61BMrmnZ1AV7IW34564l+i6g:UyMn204KYoSWlcRe4Wo
MD5:	6E7008F2FCF3B8302C49D8EF64D1E314
SHA1:	4ADBC38563820BBA4F506BBC8887EFA3D637EEC9
SHA-256:	D53BF845E8818655EE6565446DD4C5A1342E1D21CC994D78B49DF508460C0DB7
SHA-512:	86AE814933641CCF5DFDA3DC4B93B58C50F2C9D97181F933126B70C6BE7EE3A87BE852B46ABCB2F1C93D4D8A98FAE2F08A19C8CF1AF1B2B1F5A84133E0E363D4
Malicious:	false
Reputation:	low
Preview:	@...e.....p.....@.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fcnwidmg.j4k.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wrsvjmzf.aep.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpFDE9.tmp	
Process:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.142982930985104
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaPxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTqv
MD5:	235101EAAD05FEC8A207B7BB96081ED3
SHA1:	EE8454694B8F9ADF65E3A92D3FB48171ABC8ED31
SHA-256:	0F6A053C16BA89B1FA0BEA8A854E9986CD1C1E7C174080BD2384A575847228D3
SHA-512:	C464A7AFF91173EDADB14EC8192A9A316C6C7B6C79704903856EFF8E3417D893B80ABAD5D9DBCD0CC666BDD67D1CF6FC3139A12631E4DBA946E91F4312D9142
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\wKwiksScXFp.exe	
Process:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	865280
Entropy (8bit):	7.723556535295317

Encrypted:	false
SSDEEP:	24576:ixgV10PpKEXK/UUHyINBMXlc1fe9IbUDHDl:agVWhtK/5pN2Xlyf7U
MD5:	ED3E368480CE9FDD917565B149D52E14
SHA1:	D8F888CFEE5175C6D4F8DA8007BF9E92CC5F0D87
SHA-256:	3D547C5731A7C08B7D25C4724CB9AE8A75CE246DC2715EE0E58EDBB5EC2221F8
SHA-512:	8766FC1BDA8908CFE6130AF60D0FA6AF47B7F89B7BBE5B10DF0BA127EAD213905C5BDDF86EED44027445A08ED0FF5A983809F6B7C4C31E2BAE0D71EB7502F538
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..,.....K... ...`....@.. .....@.....K..W....`..... ....H.....text....+... ...,..... ..`.rsrc.....`.....@..@.rel oc.....2.....@..B.....K.....H.....X.....0.....*....0.....K...%.r...p.%.rS..p.%.ra..p.}.....}.....(.... .cO. ....a%..^E....k. .....M.....+i...(..... .c.mZ .g..a+...{.....(.....~....t.....{....(....& ...;Z Q..,a+..{.....(..... ....Z ...a8r...*....0..M..... V... .{).a%..^E.....'.....+%.(..... ..@.Z ..M.a+... ...Z D5X.a+.*....0.....*...0.....{....(.....(.....sA.....(.....(....(....(.....o9.

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

Process:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220808\PowerShell_transcript.358075.dN3uju++.20220808173030.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5793
Entropy (8bit):	5.400782329528835
Encrypted:	false
SSDEEP:	96:BZwjONYqDo1ZyZpjONYqDo1Z9rtjjZDjONYqDo1ZlyTTdZG:T
MD5:	B1B7833C5D478B84530FB1E7BB77DE47
SHA1:	249E79A212063F8E39AF6D7989BA589C652EFDE6
SHA-256:	49E4228F30F5FB7F34711DC35B143853406C949C863588D7499AD34C770BDA71
SHA-512:	A70AB104476E79B0A67F744B051E9050B7DD58DDCF1873A25900699930F30651BF48CA1567280322327EADED634F56B3048FED44B60790FDA8D8CD204A2FB294
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220808173032..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\wKwiksScXFp.exe..Process ID: 4400..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220808173032..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\wKwiksScXFp.exe..**********..Windows PowerShell transcript start..Start time: 20220808173525..Username: computer\user..RunAs User: computer\jo

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.723556535295317

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:	SwiftMessage_Unlocked_Transaction ProofMessage.exe
File size:	865280
MD5:	ed3e368480ce9fdd917565b149d52e14
SHA1:	d8f888cfee5175c6d4f8da8007bf9e92cc5f0d87
SHA256:	3d547c5731a7c08b7d25c4724cb9ae8a75ce246dc2715ee0e58edbb5ec2221f8
SHA512:	8766fc1bda8908cfe6130af60d0fa6af47b7f89b7bbe5b10df0ba127ead213905c5bddf86eed44027445a08ed0ff5a983809f6b7c4c31e2bae0d71eb7502f538
SSDEEP:	24576:ixgV10PpKEXK/UUHyINBMXlc1fe9IbUDHDl:agVWhtK/5pN2Xlyf7U
TLSH:	0A059D5BBF10324DC567A975DE4B7C61A7F22C2A322AD07A7513380E8AFF742DA11076
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..,.....K... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d4bde
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:	0x62F0FF81 [Mon Aug 8 12:20:17 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4b84	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x3a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	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	0xd2be4	0xd2c00	False	0.7859103925711743	data	7.729603877475422	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x3a8	0x400	False	0.37890625	data	2.954522289805604	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	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	0xd6058	0x34c	data		

Imports

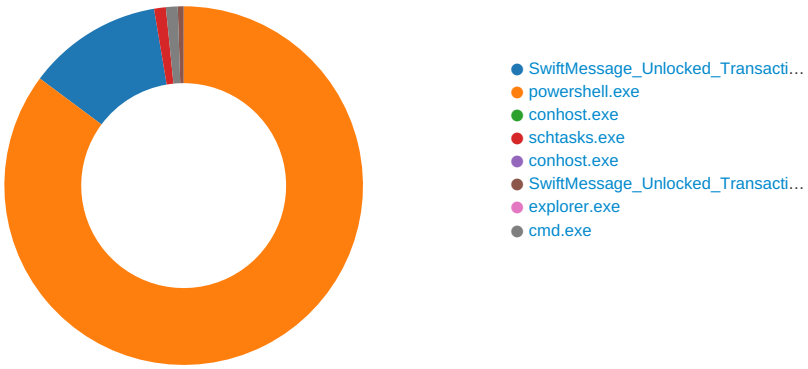
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SwiftMessage_Unlocked_Transaction ProofMessage.exe PID: 3144, Parent PID: 5972

General	
Target ID:	0
Start time:	17:30:14
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe"
Imagebase:	0xd30000
File size:	865280 bytes
MD5 hash:	ED3E368480CE9FDD917565B149D52E14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.287868209.0000000004215000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.287868209.0000000004215000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.287868209.0000000004215000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.287868209.0000000004215000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.285088525.0000000003392000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.281630024.0000000003165000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **4400**, Parent PID: **3144**

General

Target ID:	3
Start time:	17:30:28
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\wKwiksScXFp.exe
Imagebase:	0x3a0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6CD1CF06	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	6CD1CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BAC5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BAC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fcnwidmg.j4k.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wrsvjmzf.aep.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220808	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BB6BEFF	CreateDirectoryW
C:\Users\user\Documents\20220808\PowerShell_transcript.358075.dN3uju++.20220808173030.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fcnwidmg.j4k.ps1	success or wait	1	6BB66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wrsvjmzf.aep.psm1	success or wait	1	6BB66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fcnwidmg.j4k.ps1	0	1	31	1	success or wait	1	6BB61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wrsvjmzf.aep.psm1	0	1	31	1	success or wait	1	6BB61B4F	WriteFile
C:\Users\user\Documents\20220808\PowerShell_transcript.358075.dN3uju++.20220808173030.txt	0	3	ff		success or wait	1	6BB61B4F	WriteFile
C:\Users\user\Documents\20220808\PowerShell_transcript.358075.dN3uju++.20220808173030.txt	3	678	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 38 30 38 31 37 33 30 33 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 35 38 30 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220808173032Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 358075 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6BB61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 70 14 00 00 18 00 00 00 fd 0e fd 04 fd 09 fd 09 09 00 00 40 01 fd 00 0e 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@ep@@	success or wait	1	6CFE76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M?MBMDmEEMqqS%n4&5&7&	success or wait	11	6CFE76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CD01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22388	success or wait	1	6CD0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6BB61B4F	ReadFile

Analysis Process: conhost.exe PID: **3404**, Parent PID: **4400**

General

Target ID:	5
Start time:	17:30:29
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: schtasks.exe PID: **5656**, Parent PID: **3144**

General

Target ID:	6
Start time:	17:30:29
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\wKwiksScXFp" /XML "C:\Users\user\AppData\Local\Temp\tmpFDE9.tmp
Imagebase:	0xe20000
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\tmpFDE9.tmp	unknown	2	success or wait	1	E2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFDE9.tmp	unknown	1599	success or wait	1	E2ABD9	ReadFile

Analysis Process: conhost.exe PID: **3608**, Parent PID: **5656**

General

Target ID:	7
Start time:	17:30:30
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: SwiftMessage_Unlocked_Transaction ProofMessage.exe PID: **1888**, Parent PID: **3144**

General

Target ID:	8
Start time:	17:30:34
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe
Imagebase:	0xc20000
File size:	865280 bytes
MD5 hash:	ED3E368480CE9FDD917565B149D52E14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.275784202.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000000.275784202.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.275784202.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.275784202.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41B817	NtReadFile

Analysis Process: explorer.exe PID: **3616**, Parent PID: **1888**

General

Target ID:	11
Start time:	17:30:40

Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.363258923.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000000.363258923.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.363258923.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.363258923.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.382443065.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000000.382443065.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.382443065.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.382443065.000000000D6A3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2896**, Parent PID: **3616**

General

Target ID:	21
Start time:	17:31:42
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.503381407.0000000000AB0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.500415213.00000000005D0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.500415213.00000000005D0000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.500415213.00000000005D0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.500415213.00000000005D0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.503590893.0000000000AE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.503590893.0000000000AE0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.503590893.0000000000AE0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.503590893.0000000000AE0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SwiftMessage_Unlocked_Transaction ProofMessage.exe	cannot delete	1	5EB847	NtDeleteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5EB817	NtReadFile

Disassembly

No disassembly