

JOeSandbox Cloud BASIC



ID: 598602

Sample Name:

SHIPMENTDOCUMENTSPDF.exe

Cookbook: default.jbs

Time: 20:28:20

Date: 28/03/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SHIPMENTDOCUMENTSPDF.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: AveMaria	3
Yara Signatures	3
Memory Dumps	3
Unpacked PEs	4
Sigma Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
Exploits	4
Networking	4
E-Banking Fraud	4
System Summary	4
Hooking and other Techniques for Hiding and Protection	5
Anti Debugging	5
Stealing of Sensitive Information	5
Remote Access Functionality	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
World Map of Contacted IPs	8
General Information	8
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	11
Sections	11
Resources	12
Imports	12
Possible Origin	12
Network Behavior	12
Statistics	12
System Behavior	13
Analysis Process: SHIPMENTDOCUMENTSPDF.exePID: 6796, Parent PID: 5140	13
General	13
File Activities	13
File Read	13
Registry Activities	13
Disassembly	13

Windows Analysis Report

SHIPMENTDOCUMENTSPDF.exe

Overview

General Information

Sample Name:

SHIPMENTDOCUMENTSPDF.exe

Analysis ID:

598602

MD5:

db995bcbc1b1ffe..

SHA1:

95049e53f64a1b..

SHA256:

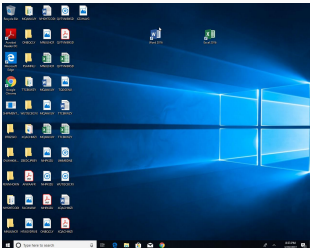
bb95fa20a55260..

Tags:

exe

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AveMaria UACMe

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

Signatures

Antivirus / Scanner detection for sub...

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected UACMe UAC Bypass...

Antivirus detection for URL or domain

Malicious sample detected (through...

Yara detected AveMaria stealer

Initial sample is a PE file and has a...

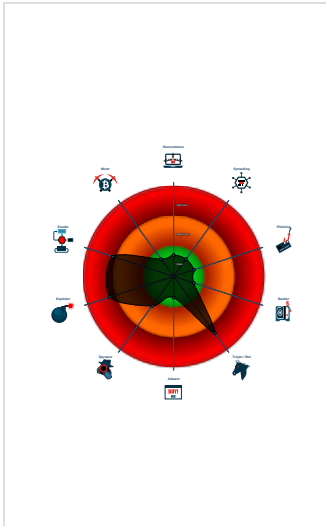
C2 URLs / IPs found in malware con...

Contains functionality to hide user a...

Found potential dummy code loops ...

Uses 32bit PE files

Classification



Process Tree

System is w10x64

 SHIPMENTDOCUMENTSPDF.exe (PID: 6796 cmdline: "C:\Users\user\Desktop\SHIPMENTDOCUMENTSPDF.exe" MD5: DB995BCBC1B1FFE95CBDE7F316B577BC)

cleanup

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "goodies.dynamic-dns.net",
  "port": 5200
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.542027781.0000000000B7F000.0000002.00001000.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0xdf0:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0xdf0:\$c1: Elevation:Administrator!new:
00000000.00000002.542027781.0000000000B7F000.0000002.00001000.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000000.00000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0x1972f:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x1972f:\$c1: Elevation:Administrator!new:

Source	Rule	Description	Author	Strings
00000000.00000002.542642008.0000000002910000.00000 040.00001000.00020000.00000000.sdmp	JoeSecurity_UAC Me	Yara detected UACMe UAC Bypass tool	Joe Security	
00000000.00000002.542642008.0000000002910000.00000 040.00001000.00020000.00000000.sdmp	JoeSecurity_Cred entialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SHIPMENTDOCUMENTSPDF.exe.29289af.3.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	0xd80:\$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.2.SHIPMENTDOCUMENTSPDF.exe.29289af.3.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0xd80:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0xd80:\$c1: Elevation:Administrator!new:
0.2.SHIPMENTDOCUMENTSPDF.exe.29289af.3.raw.unpack	JoeSecurity_UAC Me	Yara detected UACMe UAC Bypass tool	Joe Security	
0.2.SHIPMENTDOCUMENTSPDF.exe.291053f.4.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	0x191f0:\$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.2.SHIPMENTDOCUMENTSPDF.exe.291053f.4.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0x191f0:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x191f0:\$c1: Elevation:Administrator!new:
Click to see the 25 entries				

Sigma Signatures

⛔ No Sigma rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Yara detected AveMaria stealer

Exploits



Yara detected UACMe UAC Bypass tool

Networking



C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected AveMaria stealer

System Summary



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection



Contains functionality to hide user accounts

Anti Debugging



Found potential dummy code loops (likely to delay analysis)

Stealing of Sensitive Information



Yara detected AveMaria stealer

Remote Access Functionality

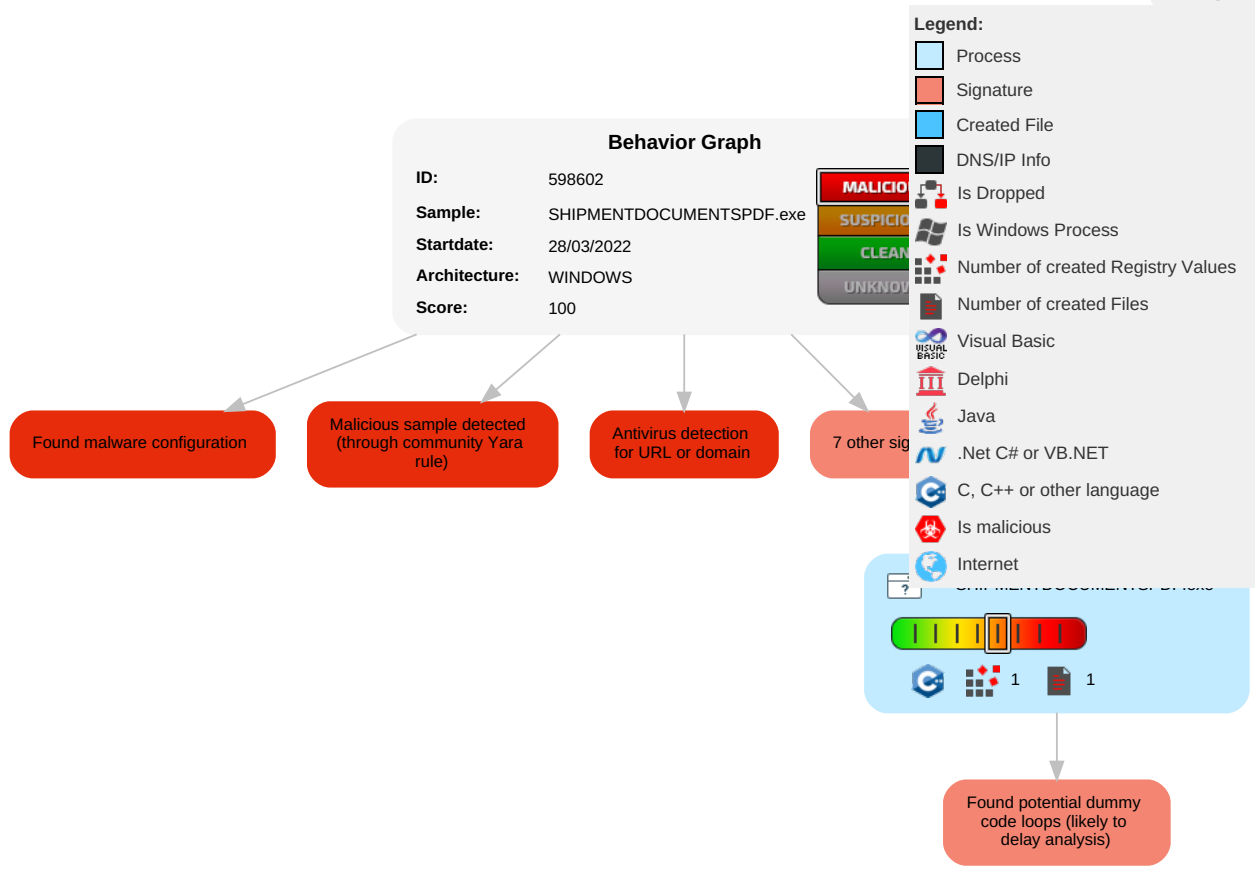


Yara detected AveMaria stealer

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	Windows Management Instrumentation	Path Interception	Path Interception	2 Masquerading	1 1 Input Capture	1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	2 System Information Discovery	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)	1 Deobfuscate/Decode Files or Information	NTDS	System Network Configuration 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 Hidden Users	LSA Secrets	Remote System 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	1 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

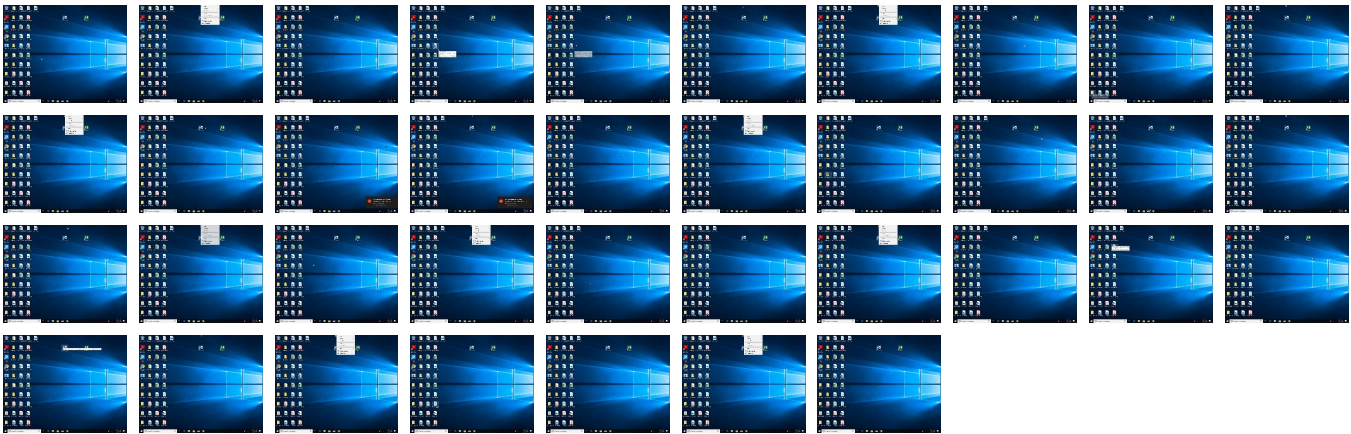
Behavior Graph



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
SHIPMENTDOCUMENTSPDF.exe	58%	Virustotal		Browse
SHIPMENTDOCUMENTSPDF.exe	24%	Metadefender		Browse
SHIPMENTDOCUMENTSPDF.exe	62%	ReversingLabs	Win32.Trojan.Ave MariaRat	
SHIPMENTDOCUMENTSPDF.exe	100%	Avira	TR/AD.MortyStealer.vctqk	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SHIPMENTDOCUMENTSPDF.exe.291053f.4.unpack	100%	Avira	TR/Patched.Ren .Gen3		Download File
0.2.SHIPMENTDOCUMENTSPDF.exe.a30000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
goodies.dynamic-dns.net	3%	Virustotal		Browse
goodies.dynamic-dns.net	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

 No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
goodies.dynamic-dns.net	true	3%, Virustotal, Browse - Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/syohex/java-simple-mine-sweeperC :	SHIPMENTDOCUMENTSPDF.exe, 00000000.0000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp, SHIPMENTDOCUMENTSPDF.exe, 00000000.00000002.541978426.0000000000A44000.00000002.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	598602
Start date and time:	2022-03-28 18:28:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SHIPMENTDOCUMENTSPDF.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@1/0@0/0
EGA Information:	Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 97.6%) • Quality average: 71.9% • Quality standard deviation: 20.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.35.228.56
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, sls.update.microsoft.com, e1723.g.akamaiedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globa.lredir.akadns.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

 No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
------------	---

Entropy (8bit):	3.945070832085131
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SHIPMENTDOCUMENTSPDF.exe
File size:	2554880
MD5:	db995bcbcb1b1ffe95cbde7f316b577bc
SHA1:	95049e53f64a1b5050d697d88ccc8bf62d58e3f6
SHA256:	bb95fa20a55260f729584b7932c7dba208dcc5b0a7597be447a72e481e0dcb09
SHA512:	c09beeab2ab7c7b65d92547f1559409012a2b1f787b4d399d8c745bf16ed2178261c64ae089582123b0111a385ba6c7d698091fe4ce72ab8af1f17a40214f120
SSDEEP:	12288:3BEnRe1ljhm1xvNkPJziiPuumDNWnr3Q5W0VI6L4qj7neunRxHfk7D4pa7+oJb:+o1ld8r2JUNJ5W0VI6L7jr/
File Content Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode....\$.M5h4.T.g.T.g.T.gf0.f.T.gf0.f.T.gf0.f.T.g.#.f.T.g.#.f.T.gf0.f.T.gf0.f.T.g.T.g.T.g.#.f.T.g.#.g.T.g.#.f.T.gRich.T.g.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x4010af
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x620E49BC [Thu Feb 17 13:12:28 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	05bdc6a6adf04eca38d0953caca5e0fa

Entrypoint Preview
Instruction
jmp 00007F12A0C903A1h
jmp 00007F12A0D0E5CCh
jmp 00007F12A0CE2B57h
jmp 00007F12A0C911D2h
jmp 00007F12A0D1813Dh
jmp 00007F12A0C96598h
jmp 00007F12A0C9C173h
jmp 00007F12A0C734BEh
jmp 00007F12A0C851F9h
jmp 00007F12A0C84644h
jmp 00007F12A0D15F2Fh
jmp 00007F12A0C9779Ah
jmp 00007F12A0CD1BE5h
jmp 00007F12A0C90320h
jmp 00007F12A0CB948Bh
jmp 00007F12A0C83D06h
jmp 00007F12A0CB4091h

Instruction
jmp 00007F12A0C7342Ch
jmp 00007F12A0CBED57h
jmp 00007F12A0CE8C5Eh
jmp 00007F12A0CC7F3Dh
jmp 00007F12A0CBE8E8h
jmp 00007F12A0C941D3h
jmp 00007F12A0C972AEh
jmp 00007F12A0CC81C9h
jmp 00007F12A0CD4A04h
jmp 00007F12A0CE98BFh
jmp 00007F12A0CD349Ah
jmp 00007F12A0C93FB5h
jmp 00007F12A0CD2530h
jmp 00007F12A0C93FBBh
jmp 00007F12A0CF6AF6h
jmp 00007F12A0CB9231h
jmp 00007F12A0C9432Ch
jmp 00007F12A0C75AC7h
jmp 00007F12A0C72E72h
jmp 00007F12A0CB3A7Dh
jmp 00007F12A0C8DC88h
jmp 00007F12A0C97283h
jmp 00007F12A0D13C9Eh

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x26b43c	0xc8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f000	0x43c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x270000	0x6004	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xfdeb0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xfea0c	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xfdee8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x26b000	0x43c	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xd1f14	0xd2000	False	0.273263113839	data	5.42725734583	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd3000	0x2e7dc	0x2e800	False	0.167485719086	data	3.57125252786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x102000	0x168e58	0x165000	False	0.111753490459	data	1.96106010749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x26b000	0x15f0	0x1600	False	0.334339488636	data	4.55588507155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x26d000	0x309	0x400	False	0.021484375	data	0.0111738187212	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.00cfg	0x26e000	0x10e	0x200	False	0.03515625	data	0.110557131259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x26f000	0x43c	0x600	False	0.182291666667	data	2.14297088193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x270000	0x7d11	0x7e00	False	0.57902405754	data	5.74904151788	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x26f170	0x17d	XML 1.0 document text	English	United States

Imports	
DLL	Import
KERNEL32.dll	HeapFree, HeapSize, GetProcessHeap, InitializeCriticalSectionEx, DeleteCriticalSection, Sleep, VirtualAlloc, VirtualProtect, FindResourceExW, LoadResource, LockResource, SizeofResource, FindResourceW, MultiByteToWideChar, WideCharToMultiByte, FreeConsole, AcquireSRWLockExclusive, AssignProcessToJobObject, CloseHandle, CompareStringW, ConnectNamedPipe, CreateDirectoryW, CreateEventW, HeapReAlloc, GetProcessId, GetProcessTimes, GetQueuedCompletionStatus, GetStartupInfoW, GetStdHandle, GetStringTypeW, GetSystemDefaultLCID, GetSystemDirectoryW, IsValidLocale, IsWow64Process, K32GetPerformanceInfo, K32GetProcessMemoryInfo, K32QueryWorkingSetEx, ReadConsoleW, ReadFile, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, SetStdHandle, HeapQueryInformation, SetEnvironmentVariableW, FreeEnvironmentStringsW, HeapAlloc, HeapDestroy, SetLastError, GetLastError, RaiseException, GetProcessHeaps, DecodePointer, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, FindClose, SetConsoleCtrlHandler, WriteConsoleW, GetFileType, EnumSystemLocalesW, GetUserDefaultLCID, GetLocaleInfoW, CreateFileW, LCMAPStringW, GetTimeFormatW, GetDateFormatW, GetCurrentThread, WriteFile, HeapValidate, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, IsDebuggerPresent, OutputDebugStringW, EnterCriticalSection, LeaveCriticalSection, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, InitializeCriticalSectionAndSpinCount, SetEvent, ResetEvent, WaitForSingleObjectEx, GetModuleHandleW, GetProcAddress, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSLISTHead, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetSystemInfo, VirtualQuery
USER32.dll	GetActiveWindow, SetProcessWindowStation, TranslateMessage, UnregisterClassW, SendMessageTimeoutW, MessageBoxW, SetProcessDPIAware, UnregisterClassA
ADVAPI32.dll	GetKernelObjectSecurity, GetAce, FreeSid, EventWrite, EventUnregister, GetLengthSid
ole32.dll	CoTaskMemRealloc, CoTaskMemFree, CoInitialize, CoUninitialize, CoCreateInstance
OLEAUT32.dll	SysAllocString, VariantCopy, SysAllocStringLen, SysFreeString, SafeArrayDestroy, VariantInit, VariantClear, VariantChangeType
SHLWAPI.dll	PathMatchSpecW
USERENV.dll	DestroyEnvironmentBlock, CreateEnvironmentBlock
VERSION.dll	VerQueryValueW, GetFileVersionInfoSizeW, GetFileVersionInfoW
WINMM.dll	timeGetTime

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior
 No network behavior found

Statistics
 No statistics

System Behavior

Analysis Process: SHIPMENTDOCUMENTSPDF.exe PID: 6796, Parent PID: 5140

General

Target ID:	0
Start time:	20:29:35
Start date:	28/03/2022
Path:	C:\Users\user\Desktop\SHIPMENTDOCUMENTSPDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SHIPMENTDOCUMENTSPDF.exe"
Imagebase:	0x10d0000
File size:	2554880 bytes
MD5 hash:	DB995BCBC1B1FFE95CBDE7F316B577BC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.542027781.0000000000B7F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.542027781.0000000000B7F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.542642008.0000000002910000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.541978426.0000000000A44000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.541978426.0000000000A44000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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\Desktop\SHIPMENTDOCUMENTSPDF.exe	unknown	2554880	success or wait	1	A41E78	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Disassembly

 No disassembly