ID: 598602
Sample Name:
SHIPMENTDOCUMENTSPDF.exe
Cookbook: default.jbs
Time: 20:37:46
Date: 28/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

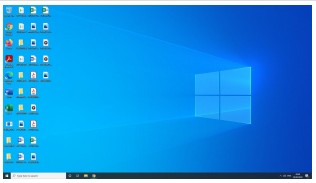
Windows Analysis Report

SHIPMENTDOCUMENTSPDF.exe

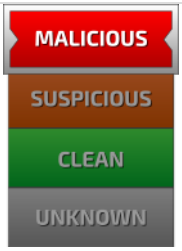
Overview

General Information

Sample Name:	SHIPMENTDOCUMENTSPDF.exe
Analysis ID:	598602
MD5:	db995bcbc1b1ffe..
SHA1:	95049e53f64a1b..
SHA256:	bb95fa20a55260..
Infos:	



Detection



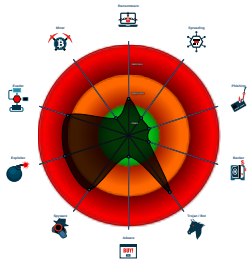
AveMaria UACMe

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected UACMe UAC Bypass…
- Antivirus detection for URL or domain
- Yara detected AveMaria stealer
- Initial sample is a PE file and has a…
- Contains functionality to hide user a…
- Contains functionality to steal e-mai…
- Contains functionality to steal Chrom…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64native**
- SHIPMENTDOCUMENTSPDF.exe (PID: 6764 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
00000002.00000002.160901038082.000000000326F000.00000002.00001000.00020000.00000000.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:
00000002.00000002.160901038082.000000000326F000.00000002.00001000.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000002.00000002.160900903714.0000000003134000.00000002.00001000.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.160900903714.0000000003134000.00000002.00001000.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.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:
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.SHIPMENTDOCUMENTSPDF.exe.27389af.1.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
2.2.SHIPMENTDOCUMENTSPDF.exe.27389af.1.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
2.2.SHIPMENTDOCUMENTSPDF.exe.27389af.1.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
2.2.SHIPMENTDOCUMENTSPDF.exe.272053f.2.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x17ff0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
2.2.SHIPMENTDOCUMENTSPDF.exe.272053f.2.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x17ff0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x17ff0:$c1: Elevation:Administrator!new:
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

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

HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject threads in other processes

Stealing of Sensitive Information

Yara detected AveMaria stealer

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality

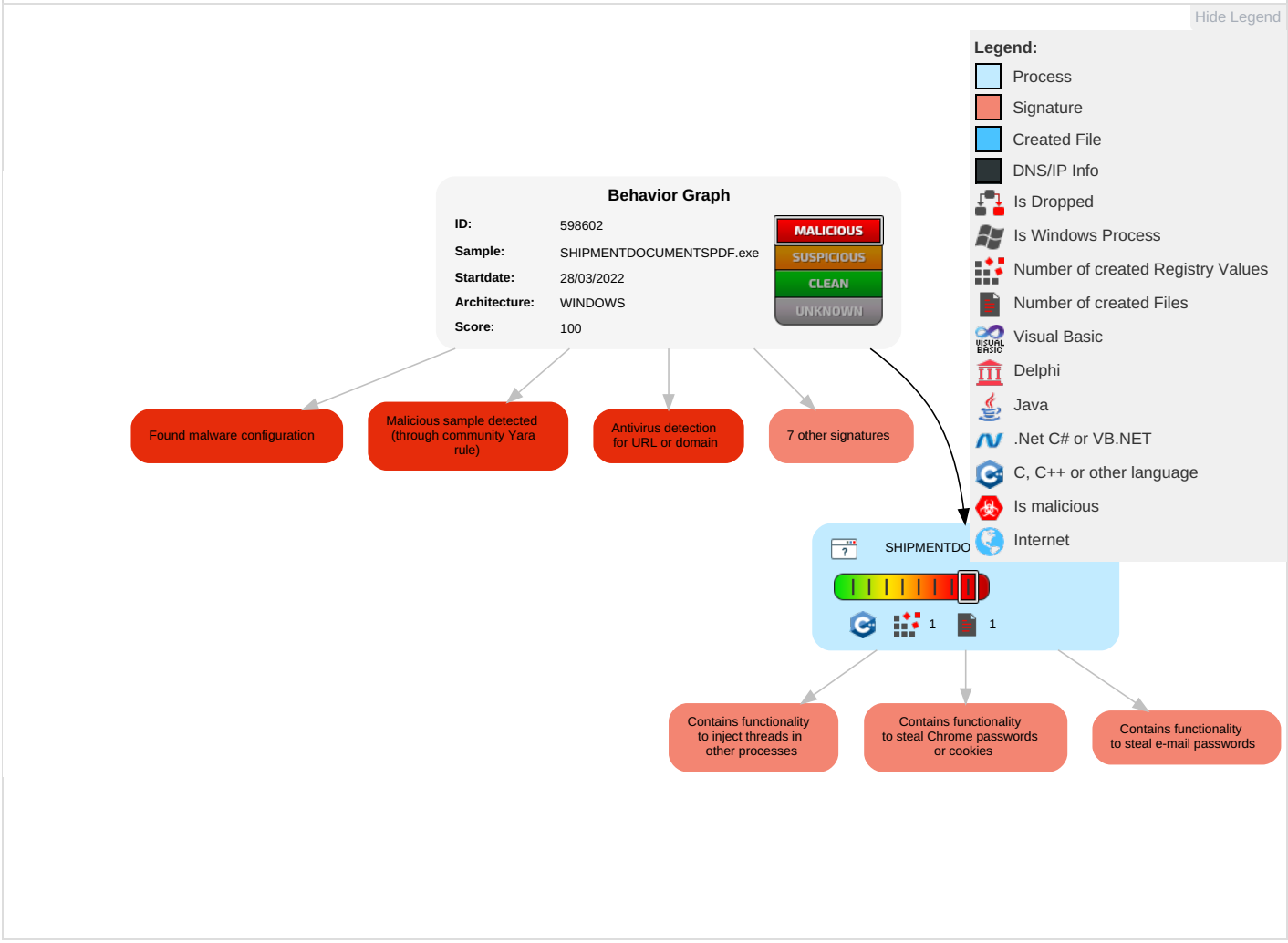
Yara detected AveMaria stealer

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	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Service Execution	1 Create Account	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 System Service Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Windows Service	1 Windows Service	2 Obfuscated Files or Information	1 Credentials In Files	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Process Injection	1 Software Packing	NTDS	1 4 System Information 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 DLL Side-Loading	LSA Secrets	2 1 Security Software 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	2 Masquerading	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Virtualization/Sandbox Evasion	DCSync	1 Process Discovery	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 Access Token Manipulation	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

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.AveMariaRat	
SHIPMENTDOCUMENTSPDF.exe	100%	Avira	TR/AD.MortyStealer.vctqk	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.SHIPMENTDOCUMENTSPDF.exe.272053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
2.2.SHIPMENTDOCUMENTSPDF.exe.3120000.3.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, 00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.sdmp, SHIPMENTDOCUMENTSPDF.exe, 00000002.00000002.160900903714.0000000003134000.00000002.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/syohex/java-simple-mine-sweeper	SHIPMENTDOCUMENTSPDF.exe	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 18:37:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 16s
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 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

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:	db995bcbc1b1ffe95cbde7f316b577bc

SHA1:	95049e53f64a1b5050d697d88ccc8bf62d58e3f6
SHA256:	bb95fa20a55260f729584b7932c7dba208dcc5b0a7597be447a72e481e0dcb09
SHA512:	c09beeab2ab7c7b65d92547f1559409012a2b1f787b4d399d8c745bf16ed2178261c64ae089582123b0111a385ba6c7d698091fe4ce72ab8af1f17a40214f120
SSDEEP:	12288:3BEnRe1ljhm1xvNkPJziiPuumDNWnr3Q5WOVI6L4qj7neunRxHfk7D4pa7+oJb:+o1ld8r2JUNJ5WOVI6L7jr/
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.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 00007F21008CDD81h
jmp 00007F210094BFACh
jmp 00007F2100920537h
jmp 00007F21008CEBB2h
jmp 00007F2100955B1Dh
jmp 00007F21008D3F78h
jmp 00007F21008D9B53h
jmp 00007F21008B0E9Eh
jmp 00007F21008C2BD9h
jmp 00007F21008C2024h
jmp 00007F210095390Fh
jmp 00007F21008D517Ah
jmp 00007F210090F5C5h
jmp 00007F21008CDD00h
jmp 00007F21008F6E6Bh
jmp 00007F21008C16E6h
jmp 00007F21008F1A71h
jmp 00007F21008B0E0Ch
jmp 00007F21008FC737h
jmp 00007F210092663Eh
jmp 00007F210090591Dh
jmp 00007F21008FC2C8h
jmp 00007F21008D1BB3h
jmp 00007F21008D4C8Eh

Instruction
jmp 00007F2100905BA9h
jmp 00007F21009123E4h
jmp 00007F210092729Fh
jmp 00007F2100910E7Ah
jmp 00007F21008D1995h
jmp 00007F210090FF10h
jmp 00007F21008D199Bh
jmp 00007F21009344D6h
jmp 00007F21008F6C11h
jmp 00007F21008D1D0Ch
jmp 00007F21008B34A7h
jmp 00007F21008B0852h
jmp 00007F21008F145Dh
jmp 00007F21008CB668h
jmp 00007F21008D4C63h
jmp 00007F210095167Eh

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
.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: 6764, Parent PID: 1444

General

Target ID:	2
Start time:	20:39:38
Start date:	28/03/2022
Path:	C:\Users\user\Desktop\SHIPMENTDOCUMENTSPDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SHIPMENTDOCUMENTSPDF.exe"
Imagebase:	0x750000
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: 00000002.00000002.160901038082.000000000326F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000002.160901038082.000000000326F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.160900903714.0000000003134000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000002.160900903714.0000000003134000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000002.160900189054.0000000002720000.00000040.00001000.00020000.00000000.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	3131E78	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