ID: 586535
Sample Name: ciao
Cookbook: default.jbs
Time: 10:51:19
Date: 10/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ciao 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: Dridex 3
Yara Signatures 3
Memory Dumps 3
Unpacked PEs 4
Sigma Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Compliance 4
Networking 4
E-Banking Fraud 4
Data Obfuscation 4
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
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 8
General Information 9
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 11
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 13
Possible Origin 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 14
DNS Queries 14
DNS Answers 14
Statistics 14
System Behavior 14
Analysis Process: ciao.exePID: 7040, Parent PID: 5024 14
General 14
File Activities 15
File Created 15
Disassembly 16

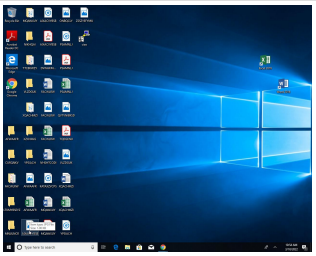
Windows Analysis Report

ciao

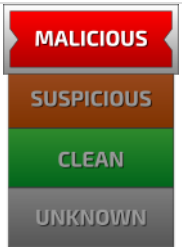
Overview

General Information

Sample Name:	ciao (renamed file extension from none to exe)
Analysis ID:	586535
MD5:	2950930fd9685a..
SHA1:	9ce522284f4ed8..
SHA256:	484573512eb4bf..
Infos:	



Detection



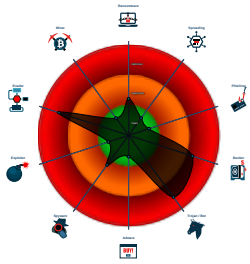
Dridex CryptOne

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Detected Dridex e-Banking trojan
- Yara detected CryptOne packer
- C2 URLs / IPs found in malware con…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Found a high number of Window / U…

Classification



Process Tree

- **System is w10x64**
- ciao.exe (PID: 7040 cmdline: "C:\Users\user\Desktop\ciao.exe" MD5: 2950930FD9685A9A7D26C965C529B60F)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 10111,
  "C2 list": [
    "172.104.87.236:1512",
    "111.230.104.169:3388",
    "103.199.16.245:1512",
    "123.206.58.135:8172"
  ],
  "RC4 keys": [
    "b58Q3DBSSKBc6NV2yyV3b42Fe6ojFZI8N0WEB",
    "v6jcviKqGv6lx4uz0Uk6jZvCxPAlfkVHiJTrTCXnmNdXSzxXzMkdiXrFRnzJTUZjrSf1W"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.695331937.00000000021F0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.695387453.0000000002240000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.694841619.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ciao.exe.2240000.1.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.ciao.exe.400000.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.ciao.exe.2240000.1.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.ciao.exe.400000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

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

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Dridex unpacked file

Detected Dridex e-Banking trojan

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Stealing of Sensitive Information

Yara detected CryptOne packer

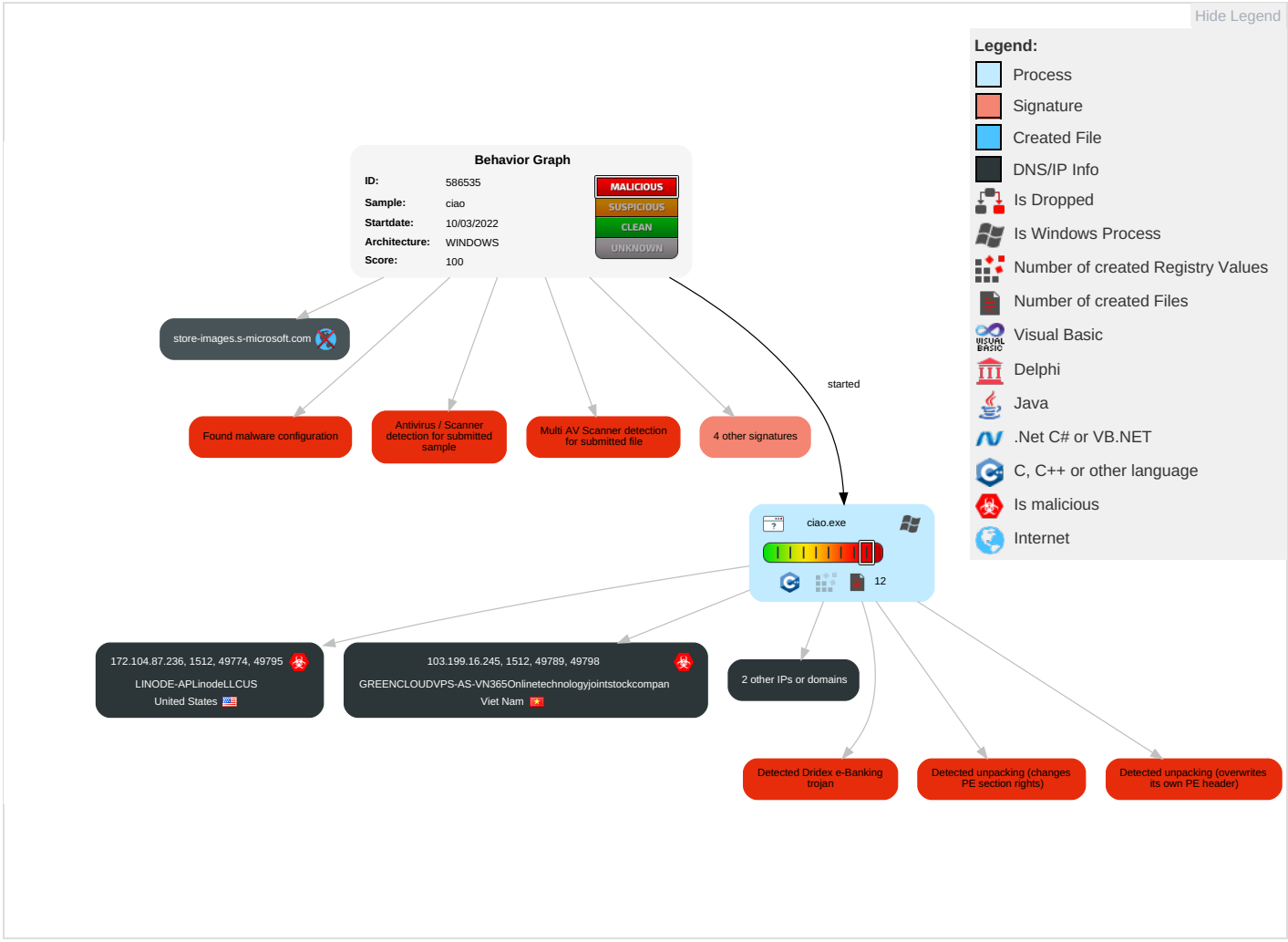
Remote Access Functionality

Yara detected CryptOne packer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	Path Interception	1 Virtualization/Sandbox Evasion	OS Credential Dumping	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Obfuscated Files or Information	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 2 Software Packing	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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)	Binary Padding	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User 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	Steganography	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 File and Directory 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	Indicator Removal from Tools	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

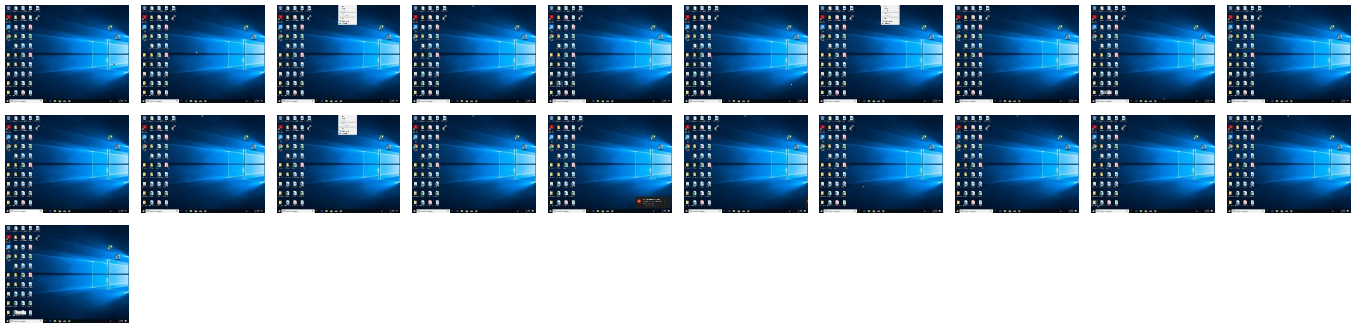
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ciao.exe	32%	Metadefender		Browse
ciao.exe	93%	ReversingLabs	Win32.Infostealer.Dridex	
ciao.exe	100%	Avira	HEUR/AGEN.1219116	
ciao.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.ciao.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1219116		Download File
0.2.ciao.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234144		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://123.206.58.135:8172/h	0%	Avira URL Cloud	safe	

Domains and IPs

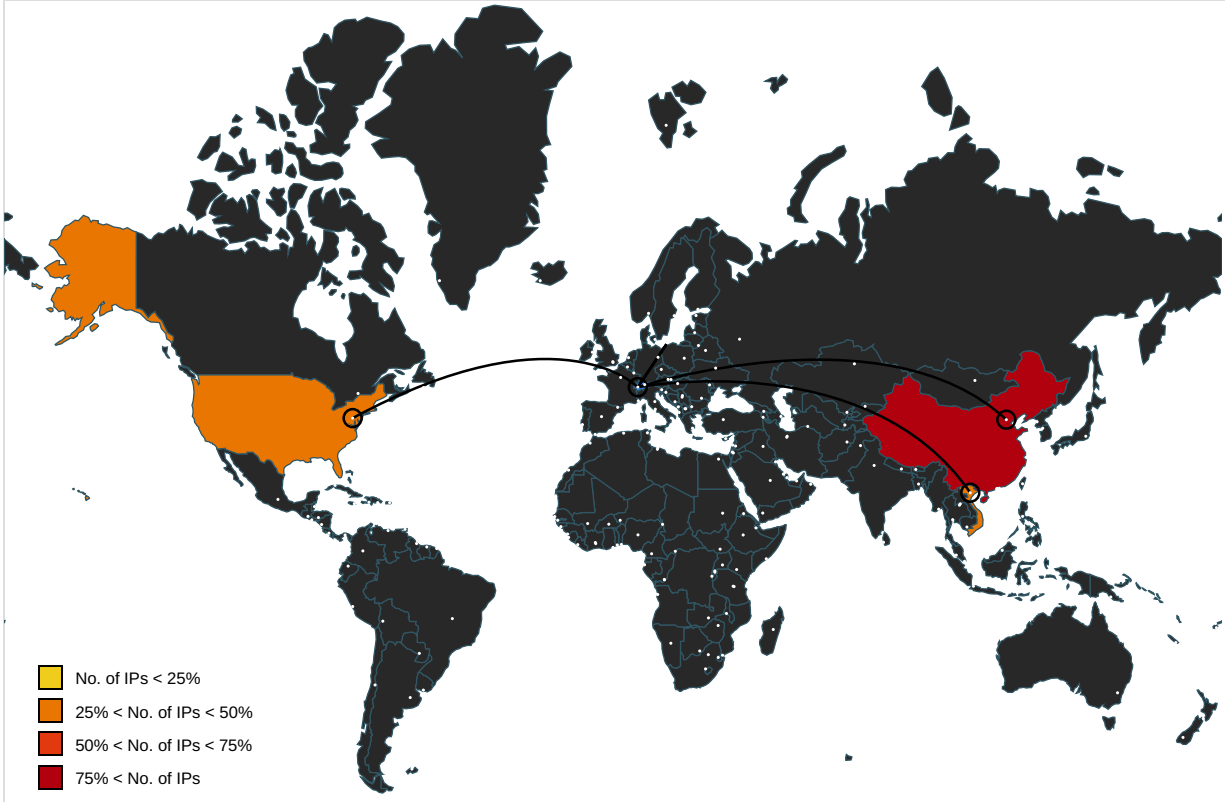
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
store-images.s-microsoft.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://123.206.58.135:8172/h	ciao.exe, 00000000.00000002.694824738.00000000009D000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
123.206.58.135	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	true
103.199.16.245	unknown	Viet Nam		63734	GREENCLOUDVPS-AS-VN365Onlinetechnologyjointstockcompan	true
111.230.104.169	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	true
172.104.87.236	unknown	United States		63949	LINODE-APLinodeLLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	586535
Start date:	10.03.2022
Start time:	10:51:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ciao (renamed file extension from none to 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:	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.bank.troj.evad.winEXE@1/0@1/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3.9% (good quality ratio 3.9%) • Quality average: 78.9% • Quality standard deviation: 16%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.5.146, 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e16646.dscg.akamaiedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, storeedgefd.xbetservices.akadns.net, storeedgefd.dsx.mp.microsoft.com
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: ciao.exe

Simulations

Behavior and APIs

Time	Type	Description
10:52:57	API Interceptor	7x Sleep call for process: ciao.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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.108652688508333
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ciao.exe
File size:	466432
MD5:	2950930fd9685a9a7d26c965c529b60f
SHA1:	9ce522284f4ed862d0815968c91451f074b85e81
SHA256:	484573512eb4bf8cbfd85c4b209bc12bfc17cd873d733cfc4b49ce13914b9443
SHA512:	fc69da1dfef82ea8d74811a5296e24ccc11eedf98421d44eefcf9e89132642befdfc6d06c43a8a98bcbab9b83c9557b1570f6ee89c58f525a9840c648e828f27
SSDEEP:	6144:we9ZfcAcig3SuEE/UPTYkkK795PuBSciRzWpIOiM35e9ZOe9ZDe9Z:bEfh3SW/Uc5K73PuBMR37p6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...=a._.....2.....t.....T.....p....@.....P.....

File Icon

Icon Hash:	c092d090bc0d990b

Static PE Info

General

Entrypoint:	0x4454e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED

DLL Characteristics:	
Time Stamp:	0x5FD2613D [Thu Dec 10 17:56:13 2020 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:	eba97c0a4b1876634a464e9c065450fb

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 4Ch
mov dword ptr [ebp-04h], 00000000h
push 0046D354h
call dword ptr [0046D680h]
mov dword ptr [0046DC60h], 00000000h
jmp 00007FDBDC71609Fh
mov eax, dword ptr [0046DC60h]
add eax, 01h
mov dword ptr [0046DC60h], eax
cmp dword ptr [0046DC60h], 0000107Fh
jnc 00007FDBDC71609Ah
call dword ptr [0046D670h]
jmp 00007FDBDC716071h
push 0046D36Ch
call dword ptr [0046D684h]
call dword ptr [0046D578h]
cmp eax, 02h
je 00007FDBDC716099h
xor eax, eax
jmp 00007FDBDC716F82h
call 00007FDBDC715FFEh
cmp dword ptr [ebp-04h], 00000000h
je 00007FDBDC7160A4h
push 0000231Eh
push 0000231Eh
call 00007FDBDC715F19h
add esp, 08h
cmp dword ptr [ebp-04h], 00000000h
je 00007FDBDC7160A4h
push 0000231Eh
push 0000231Eh
call 00007FDBDC715F01h
add esp, 08h
cmp dword ptr [ebp-04h], 00000000h
je 00007FDBDC7160A4h
push 0000231Eh
push 0000231Eh
call 00007FDBDC715EE9h
add esp, 08h
mov dword ptr [0046DC60h], 00000000h
jmp 00007FDBDC7160A1h
mov ecx, dword ptr [0046DC60h]
add ecx, 01h
mov dword ptr [0000DC60h], ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6d3a4	0x78	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x73000	0x14c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x6d564	0x148	.data
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	0x454f7	0x45600	False	0.843774634009	data	7.42644876953	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x47000	0x1c2	0x200	False	0.5859375	data	4.23847909032	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.text3	0x48000	0x1adb0	0x1ae00	False	0.0012082122093	data	0.00862531644872	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.text2	0x63000	0x4e20	0x5000	False	0.59052734375	data	5.00603909334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x68000	0x5cc0	0x5e00	False	0.580119680851	data	5.33430480294	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data3	0x6e000	0x4e20	0x5000	False	0.59052734375	data	5.00603909334	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x73000	0x14c8	0x1600	False	0.25390625	data	2.95023024978	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x731d8	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x73300	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 202099788, next used block 35015	English	United States
RT_ICON	0x735e8	0x668	data	English	United States
RT_ICON	0x73c50	0xb0	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x73d00	0x130	data	English	United States
RT_ICON	0x73e30	0x330	data	English	United States
RT_GROUP_ICON	0x74160	0x5a	data	English	United States
RT_VERSION	0x741bc	0x30c	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetCurrentProcessId, Sleep, GetTickCount, CloseHandle, OpenMutexW, GetLastError, FlushFileBuffers, CreateFileA, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, GetProcAddress, GetModuleFileNameW, GetCurrentThreadId, WriteFile, SetFilePointer, GetCurrentProcess, CreateMutexW, ReleaseMutex, TerminateProcess, InterlockedDecrement, GetModuleHandleW, LoadLibraryA, RaiseException, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSection, DeleteCriticalSection, HeapDestroy, HeapAlloc, HeapFree, HeapReAlloc, HeapSize, GetProcessHeap, InterlockedIncrement, WideCharToMultiByte, InterlockedExchange, MultiByteToWideChar, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetStartupInfoW, RtlUnwind, LCMapStringA, LCMapStringW, GetCPInfo, GetStringTypeW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, ExitProcess, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsW, GetEnvironmentStringsW, LocalAlloc, QueryPerformanceCounter, FormatMessageA, LocalFree, SetConsoleCtrlHandler, SetThreadUILanguage, GetModuleHandleA, VirtualAlloc

DLL	Import
USER32.dll	LoadCursorA, GetForegroundWindow
GDI32.dll	GetEnhMetaFileA, RealizePalette, AddFontResourceW, GetEnhMetaFileW, StrokePath, SwapBuffers, GetEnhMetaFileBits, GetStockObject
ADVAPI32.dll	RegOpenKeyW
IMM32.dll	ImmDisableIME

Version Infos

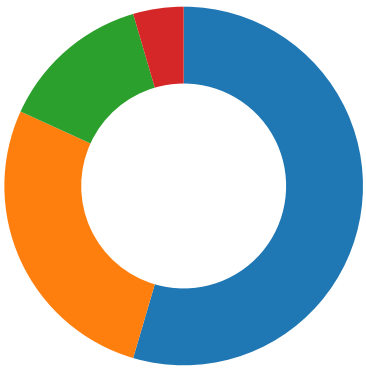
Description	Data
LegalCopyright	Copyright 1997-2017 Simon Tatham.
InternalName	PSFTP
FileVersion	Release 0.68
CompanyName	Simon Tatham
ProductName	PuTTY suite
ProductVersion	Release 0.68
FileDescription	Command-line interactive SFTP client
OriginalFilename	PSFTP
Translation	0x0809 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 10:52:56.089411974 CET	49774	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:52:56.343377113 CET	1512	49774	172.104.87.236	192.168.2.5
Mar 10, 2022 10:52:56.931067944 CET	49774	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:52:57.185810089 CET	1512	49774	172.104.87.236	192.168.2.5
Mar 10, 2022 10:52:57.821815968 CET	49774	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:52:58.075697899 CET	1512	49774	172.104.87.236	192.168.2.5
Mar 10, 2022 10:52:58.217005014 CET	49780	3388	192.168.2.5	111.230.104.169
Mar 10, 2022 10:53:01.368940115 CET	49780	3388	192.168.2.5	111.230.104.169

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 10:53:07.369541883 CET	49780	3388	192.168.2.5	111.230.104.169
Mar 10, 2022 10:53:19.499452114 CET	49789	1512	192.168.2.5	103.199.16.245
Mar 10, 2022 10:53:19.741199970 CET	1512	49789	103.199.16.245	192.168.2.5
Mar 10, 2022 10:53:20.370549917 CET	49789	1512	192.168.2.5	103.199.16.245
Mar 10, 2022 10:53:26.386729956 CET	49789	1512	192.168.2.5	103.199.16.245
Mar 10, 2022 10:53:38.523582935 CET	49793	8172	192.168.2.5	123.206.58.135
Mar 10, 2022 10:53:41.522963047 CET	49793	8172	192.168.2.5	123.206.58.135
Mar 10, 2022 10:53:47.523423910 CET	49793	8172	192.168.2.5	123.206.58.135
Mar 10, 2022 10:53:59.642584085 CET	49795	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:53:59.909619093 CET	1512	49795	172.104.87.236	192.168.2.5
Mar 10, 2022 10:54:00.415230989 CET	49795	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:54:00.682101965 CET	1512	49795	172.104.87.236	192.168.2.5
Mar 10, 2022 10:54:01.196469069 CET	49795	1512	192.168.2.5	172.104.87.236
Mar 10, 2022 10:54:01.463325024 CET	1512	49795	172.104.87.236	192.168.2.5
Mar 10, 2022 10:54:01.581051111 CET	49796	3388	192.168.2.5	111.230.104.169
Mar 10, 2022 10:54:04.587357998 CET	49796	3388	192.168.2.5	111.230.104.169
Mar 10, 2022 10:54:10.666049004 CET	49796	3388	192.168.2.5	111.230.104.169
Mar 10, 2022 10:54:22.799479961 CET	49798	1512	192.168.2.5	103.199.16.245
Mar 10, 2022 10:54:23.012582064 CET	1512	49798	103.199.16.245	192.168.2.5
Mar 10, 2022 10:54:23.526457071 CET	49798	1512	192.168.2.5	103.199.16.245
Mar 10, 2022 10:54:23.739654064 CET	1512	49798	103.199.16.245	192.168.2.5
Mar 10, 2022 10:54:24.245239019 CET	49798	1512	192.168.2.5	103.199.16.245

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 10:52:25.026051998 CET	54322	53	192.168.2.5	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 10, 2022 10:52:25.026051998 CET	192.168.2.5	8.8.8.8	0x26f6	Standard query (0)	store-images.s-microsoft.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 10, 2022 10:52:25.047528982 CET	8.8.8.8	192.168.2.5	0x26f6	No error (0)	store-images.s-microsoft.com	store-images.s-microsoft.com-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Statistics

No statistics

System Behavior

Analysis Process: ciao.exe PID: **7040**, Parent PID: **5024**

General

Target ID:	0
Start time:	10:52:31
Start date:	10/03/2022
Path:	C:\Users\user\Desktop\ciao.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ciao.exe"

Imagebase:	0x400000
File size:	466432 bytes
MD5 hash:	2950930FD9685A9A7D26C965C529B60F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000000.00000002.695331937.00000000021F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.695387453.0000000002240000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.694841619.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	43390E	HttpSendRequestW

Disassembly

No disassembly