ID: 247208
Sample Name:
citadel_1.3.3.3.vir
Cookbook: default.jbs
Time: 00:07:52
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

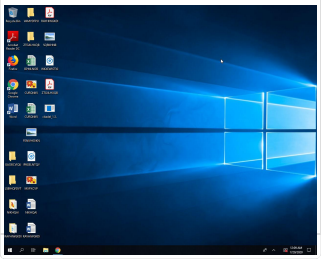
Analysis Report citadel_1.3.3.3.vir

Overview

General Information

Sample Name:	citadel_1.3.3.3.vir (renamed file extension from vir to exe)
Analysis ID:	247208
MD5:	50854eb699adde..
SHA1:	24e47df1ca6df38..
SHA256:	deb51e50b46285..

Most interesting Screenshot:



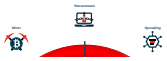
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected ZeusVM e-Banking Trojan
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Contains VNC / remote desktop func…
- Machine Learning detection for samp…
- PE file has a writeable .text section
- Antivirus or Machine Learning detec…
- Contains functionality to dynamically…
- Contains functionality to enumerate …

Classification



Startup

- **System is w10x64**
- citadel_1.3.3.3.exe (PID: 5148 cmdline: 'C:\Users\user\Desktop\citadel_1.3.3.3.exe' MD5: 50854EB699ADDE84C0106AC46D7859E5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.771080116.0000000000400000.00000040.00020000.sdmp	citadel13xy	Citadel 1.5.x.y trojan banker	Jean-Philippe Teissier / @Jipe_	• 0x75cc:$c: %BOTID% • 0x75d4:$d: %BOTNET% • 0x6b24:$e: cit_video.module • 0x1898:$ggurl: http://www.google.com/webhp
Process Memory Space: citadel_1.3.3.3.exe PID: 5148	citadel13xy	Citadel 1.5.x.y trojan banker	Jean-Philippe Teissier / @Jipe_	• 0x2bb2:$c: %BOTID% • 0x6c27:$c: %BOTID% • 0x93a7:$c: %BOTID% • 0x9580:$c: %BOTID% • 0x2bda:$d: %BOTNET% • 0x6c14:$d: %BOTNET% • 0x93bb:$d: %BOTNET% • 0x9587:$d: %BOTNET% • 0x1cdb:$e: cit_video.module • 0x8971:$e: cit_video.module • 0x8ba8:$e: cit_video.module • 0x80f:$ggurl: http://www.google.com/webhp • 0x5ce1:$ggurl: http://www.google.com/webhp • 0x7c8f:$ggurl: http://www.google.com/webhp • 0x7cdf:$ggurl: http://www.google.com/webhp

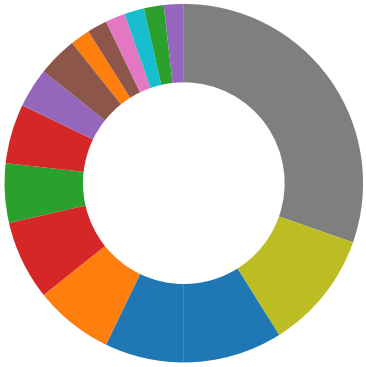
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.citadel_1.3.3.3.exe.400000.0.raw.unpack	citadel13xy	Citadel 1.5.x.y trojan banker	Jean-Philippe Teissier / @Jipe_	• 0x75cc:$c: %BOTID% • 0x75d4:$d: %BOTNET% • 0x6b24:$e: cit_video.module • 0x1898:$ggurl: http://www.google.com/webhp
0.2.citadel_1.3.3.3.exe.400000.0.unpack	citadel13xy	Citadel 1.5.x.y trojan banker	Jean-Philippe Teissier / @Jipe_	• 0x69cc:$c: %BOTID% • 0x69d4:$d: %BOTNET% • 0x5f24:$e: cit_video.module • 0xc98:$ggurl: http://www.google.com/webhp

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

System Summary:

Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

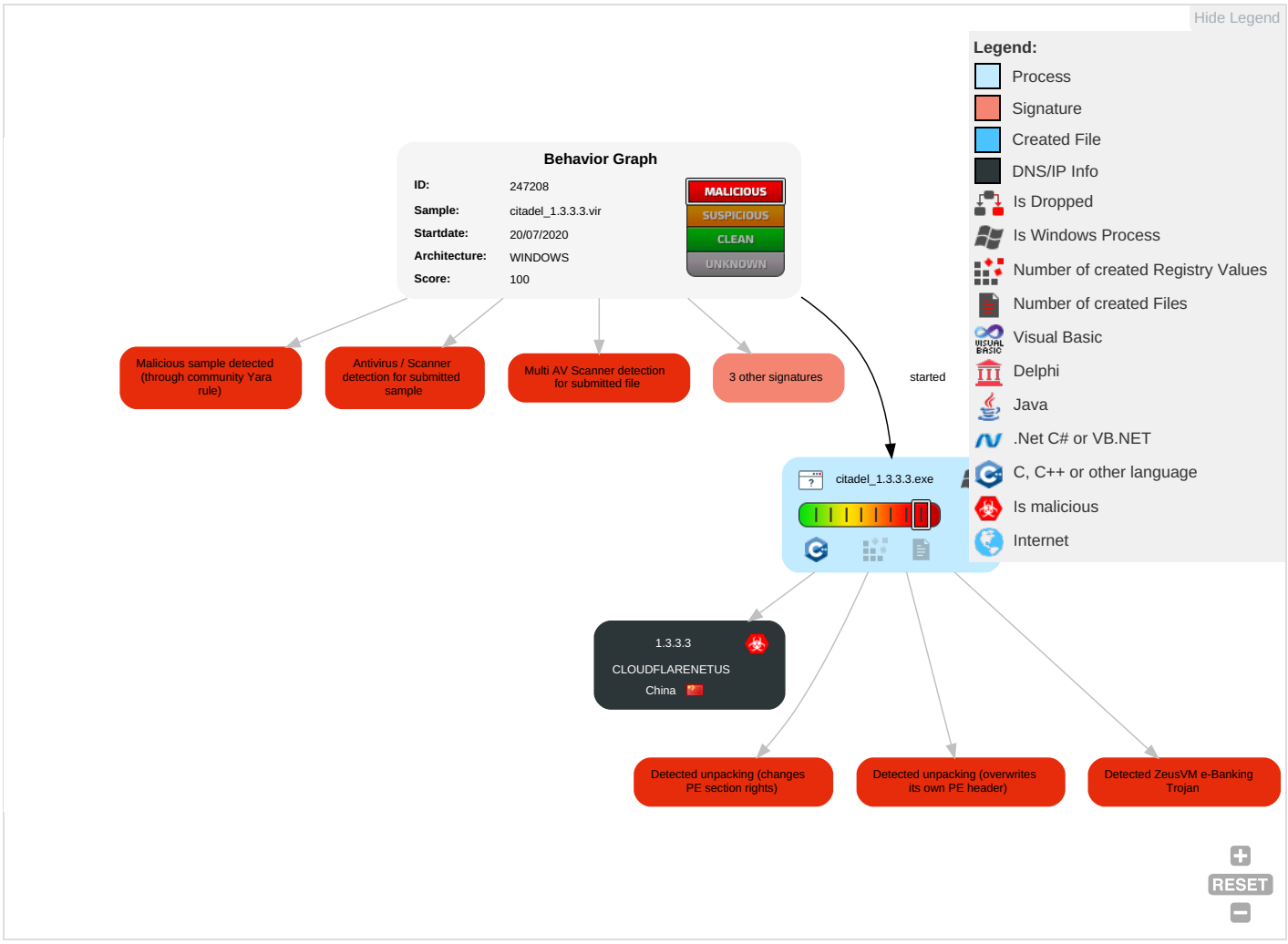
Remote Access Functionality:

Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts 1	Execution through API 1	Create Account 1	Valid Accounts 1	Software Packing 2 2	Input Capture 1 1	System Time Discovery 2	Remote File Copy 1	Input Capture 1 1	Data Encrypted 1	Commonly Used Port 1	E I N C
Replication Through Removable Media	Graphical User Interface 1	Valid Accounts 1	Access Token Manipulation 1 1	Obfuscated Files or Information 2	Network Sniffing	Account Discovery 1	Remote Desktop Protocol 1	Clipboard Data 1	Exfiltration Over Other Network Medium	Remote File Copy 1	E F C
External Remote Services	Windows Management Instrumentation	Application Shimming 1	Application Shimming 1	Valid Accounts 1	Input Capture	Security Software Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Cryptographic Protocol 2	E T L
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Virtualization/Sandbox Evasion 1	Credentials in Files	File and Directory Discovery 2	Logon Scripts	Input Capture	Data Encrypted	Remote Access Tools 1	S S
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Access Token Manipulation 1 1	Account Manipulation	System Information Discovery 1 3	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	N D C
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Install Root Certificate 1	Brute Force	Network Share Discovery 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	J D S
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	DLL Side-Loading 1	Two-Factor Authentication Interception	Virtualization/Sandbox Evasion 1	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	F A
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Indicator Blocking	Bash History	Process Discovery 1	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	D I F
Supply Chain Compromise	Rundll32	DLL Search Order Hijacking	Service Registry Permissions Weakness	Process Injection	Input Prompt	System Owner/User Discovery 1	Windows Admin Shares	Automated Collection	Exfiltration Over Physical Medium	Multilayer Encryption	F E

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
citadel_1.3.3.3.exe	87%	Virustotal		Browse
citadel_1.3.3.3.exe	74%	Metadefender		Browse
citadel_1.3.3.3.exe	92%	ReversingLabs	Win32.Trojan.Zbot	
citadel_1.3.3.3.exe	100%	Avira	TR/Crypt.XPACK.Gen	
citadel_1.3.3.3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.citadel_1.3.3.3.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.citadel_1.3.3.3.exe.a70000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.citadel_1.3.3.3.exe.a00000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.citadel_1.3.3.3.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

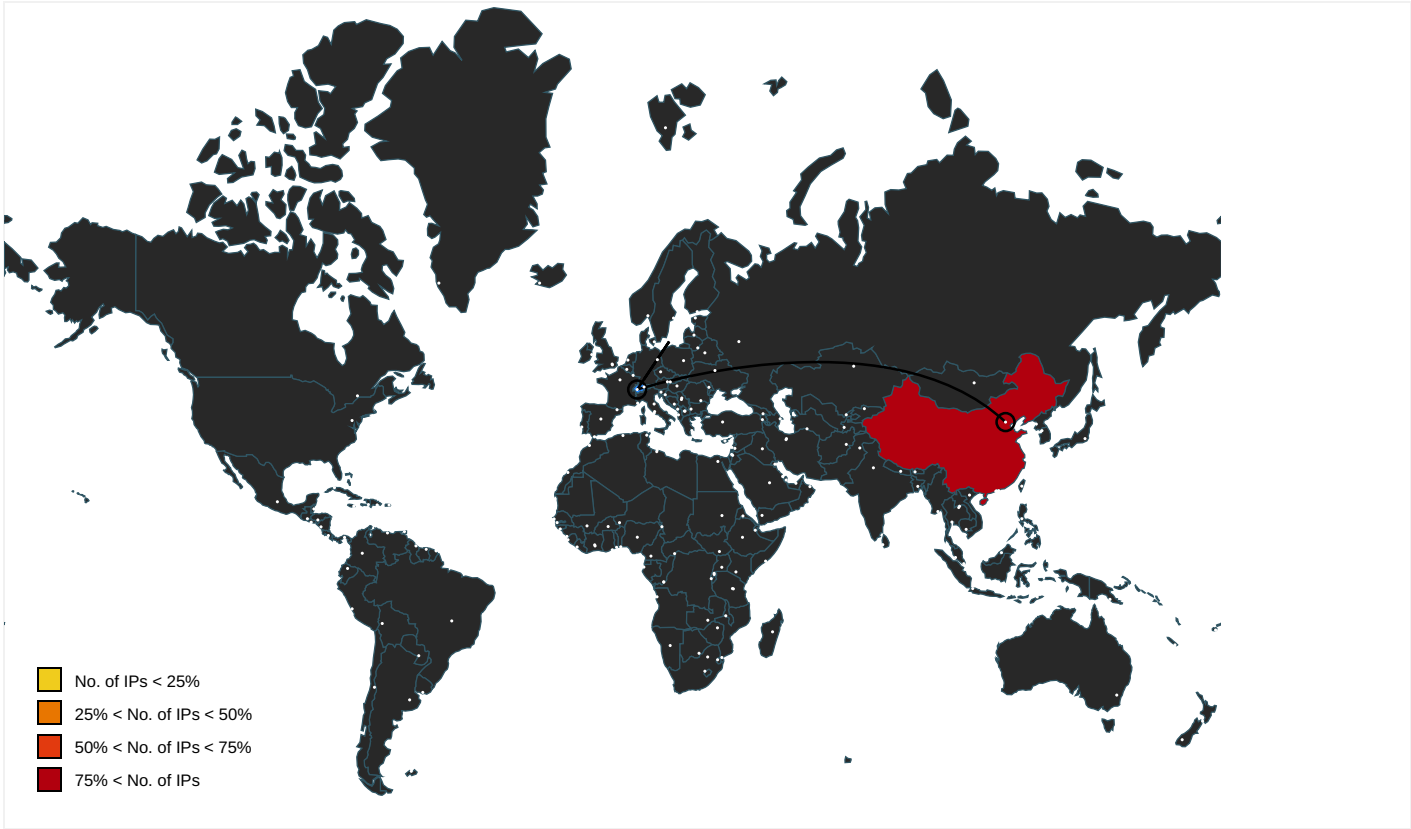
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://-%BOTID%%BOTNET%HTTP/1.0HostContent-LengthUser-AgentRefererContent-TypeAuthorization	citadel_1.3.3.3.exe, 00000000.00000002.771080116.00000000040000.00000040.00020000.sdmp	false		low

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.3.3.3	China		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247208
Start date:	20.07.2020
Start time:	00:07:52
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 3m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	citadel_1.3.3.3.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	1
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@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 52.8% (good quality ratio 48.3%) • Quality average: 80.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://comtechadsl.com/ehepsqm.exe	Get hash	malicious	Browse	• 104.20.74.28
	http://blueeyeswebsite.com/	Get hash	malicious	Browse	• 104.24.110.109
	ATT20893.HTML	Get hash	malicious	Browse	• 104.16.133.229
	ATT84128.HTML	Get hash	malicious	Browse	• 104.16.133.229
	http://https://bit.ly/30cSl6K	Get hash	malicious	Browse	• 104.16.124.96
	http://https://jhmetalinc-my.sharepoint.com/:o:/p/office/EiJ0PCnWDtJHiWQIXRi7bWgB6cFzFQtLhcLET3v8d3NRLA?rtime=ORiHa4Eq2Eg	Get hash	malicious	Browse	• 104.16.132.229
	ATT39268.HTM	Get hash	malicious	Browse	• 104.16.133.229

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment730.xls	Get hash	malicious	Browse	• 104.27.180.83
	http://atcsagacity.com/wp-admin/MYWZIKG/eigyho/s9w0816332646203713g44z0n2u/	Get hash	malicious	Browse	• 172.67.186.191
	http://https://gogoanime1.net/.well-known/acme-challenge/bid/login.php	Get hash	malicious	Browse	• 104.16.132.229
	http://https://lroetrgpfxciziew.frb.io/?bbre=pdsi93reodfxci	Get hash	malicious	Browse	• 104.16.133.229
	http://mapfrecomercial.com/	Get hash	malicious	Browse	• 104.16.202.237
	http://https://event.on24.com/wcc/r/2462461/BB0A869CCD07459AE0E4C73F0AD810E3/1209023?partnerref=connect	Get hash	malicious	Browse	• 104.17.71.206
	http://https://u10500736.ct.sendgrid.net/ls/click?upn=GJ-2Fwg0v0GjXICnjOzCZwjhkRw9-2BbFlj0p-2BETjV5NQUzZanQeaYMDpzIDJ401Kach0E7I_YxCxpoge33FNHhRVcK23d3jJCq3cIHwc-2BD1XeO3y4vWhDSyEnUs6U-2FsQ3r28LvMmBf0-2FyPTfw7LkuX8KPrqtuiBKVLJGudFG5cgos-2FYMheOpZ3KzgDMXMKE-2BA6yiT-2Bi5BQtK80dm1zrijWZnCRa6hF0zjqp3QnkLp0NHHccLK9ZW3lYLn1ntwPI5yxeaqK-2FwMj6c4bzGzF8lmQMxhNRSLY2oartjGJW1716gR3wWT6FnAMuuMr-2BmVOWIDO3doJzx	Get hash	malicious	Browse	• 104.22.0.232
	http://youbue.com	Get hash	malicious	Browse	• 104.20.21.239
	MuMuInstaller_1.1.0.4_a2ca17_yxmrfz_zh-Hans_1573441614.exe	Get hash	malicious	Browse	• 1.1.0.4
	Invoice2867.hTMl	Get hash	malicious	Browse	• 104.27.165.84
	http://https://www.seat26.com/wp-includes/js/tinymce/plugins/colorpicker/gastblogg/warenkorb.php?street=kqh1sdty120gb0c&face=guess&window=section	Get hash	malicious	Browse	• 104.16.132.229
	http://www.hobbyfarms.com/how-to-build-a-vermin-proof-chicken-feeder/	Get hash	malicious	Browse	• 104.18.99.60
	Scanned_from_Xerox_Multifunction.htm	Get hash	malicious	Browse	• 104.16.133.229

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):	7.790312227005969
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	citadel_1.3.3.3.exe
File size:	206848
MD5:	50854eb699adde84c0106ac46d7859e5
SHA1:	24e47df1ca6df385e6ee7e47ae3ba3efee8713f5
SHA256:	deb51e50b4628567f8690316317083aa337b10d9a23cbb5d8a21b6d6e8e194f
SHA512:	7594ce07af47ca63f8764b15fc1e4f7872bcd3a3f50ff02ed0d2db078f24040c3cb76763117b174f711db859b44289860382a28096b783d96de7ba188c108c9
SSDEEP:	3072:Xensktxb2UhshMtK6DQjhjoooStUl/Mes50MxQVO92KoPRYuvOJ:S92utK6DQFooofl0eLM+VO92XxO

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6.S.r{.~r{=.r{=.....p|=.v~<.x{=..s.~w{.....|{=.i...s{=.i...s{=.i...s{=.....PE..L...B. O.....P.....84.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4028c9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	
Time Stamp:	0x4F20ED42 [Thu Jan 26 06:05:54 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	8f046b399770881ff9411e404978ab69

Entrypoint Preview

Instruction
adc ecx, 00003982h
push ebp
mov ebp, esp
sub esp, 0Ch
not dword ptr [00439488h]
push dword ptr [0040A324h]
sub dword ptr [00409414h], 0040779Ch
call dword ptr [00439124h]
test eax, eax
mov dword ptr [00409418h], 00003874h
je 00007F11A8918B83h
neg dword ptr [00439494h]
xor eax, eax
jmp 00007F11A8918DC7h
push 00000014h
push 00000000h
xor dword ptr [00407778h], 00007ACCh
push 00000000h
xor dword ptr [00402DBCh], 00409448h
push 36521332h
call 00007F11A891756Ah
cmp eax, 03828795h
jne 00007F11A8918B3Ah
mov dword ptr [ebp-08h], 0DF2EFDBh
add dword ptr [00439488h], 00003A08h
mov dword ptr [ebp-08h], 0DF2EFD8h
xor dword ptr [00402DA8h], 00006E02h
mov dword ptr [ebp-04h], F54A1899h
and dword ptr [00402DACh], 0043948Ch

Instruction
lea eax, dword ptr [ebp-0Ch]
add dword ptr [00409454h], 00409450h
mov dword ptr [ebp-08h], eax
add dword ptr [00407794h], 00409444h
lea eax, dword ptr [ebp+04h]
add dword ptr [00000000h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x8000	0x55	.etab
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6000	0x8c	.itab
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3949c	0x287e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	0x53c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa52c	0x1c	.data
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	0x0	0x0	
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	0x4e80	0x5000	False	0.6322265625	data	6.86742796425	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itab	0x6000	0x17d0	0x1800	False	0.521809895833	data	5.34591850889	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.etab	0x8000	0x55	0x200	False	0.15625	data	0.976474923998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.input	0x9000	0x480	0x600	False	0.777994791667	data	6.47917282929	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0xa000	0x2eedb	0x800	False	0.6552734375	data	5.66323688931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x39000	0x2a47a	0x2a600	False	0.928863615413	data	7.82866462007	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x64000	0x554	0x600	False	0.787760416667	data	6.20147915652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x395cc	0xa98	data	English	United States
RT_CURSOR	0x3a064	0xb6c	data	English	United States
RT_BITMAP	0x3abd0	0x8d2	PC bitmap, Windows 3.x format, 25 x 29 x 24	English	United States
RT_BITMAP	0x3b4a2	0x396	PC bitmap, Windows 3.x format, 16 x 18 x 24	English	United States
RT_BITMAP	0x3b838	0x4e2	PC bitmap, Windows 3.x format, 30 x 13 x 24	English	United States

Imports

DLL	Import
SHLWAPI.dll	StrToIntW
comdlg32.dll	GetSaveFileNameA, PrintDlgExW, GetFileTitleW, FindTextW, GetOpenFileNameW

DLL	Import
KERNEL32.dll	RegisterWaitForSingleObject, SetupComm, FlushFileBuffers, FoldStringW, IsBadReadPtr, SetErrorMode, GetLocalTime, GetBinaryTypeW, CreateEventA, FindClose, GlobalLock, GetCurrentThread, SetLastError, LoadLibraryA, CreateEventW, HeapFree, GetCommConfig, TerminateThread, FindResourceExW, IsBadWritePtr, GlobalUnlock, lstrcpynW, ClearCommError, LocalAlloc, SetUnhandledExceptionFilter, MoveFileA, SetEvent, LCMapStringA, CloseHandle, OutputDebugStringA, UnhandledExceptionFilter, FindNextFileA, TlsFree, DuplicateHandle, EnumResourceLanguagesA, GetWindowsDirectoryW, OpenSemaphoreW, MoveFileExW, CreateRemoteThread, SuspendThread, FileTimeToSystemTime, SetThreadAffinityMask, GetSystemWindowsDirectoryW, CreateNamedPipeA, FindResourceW, OpenFile, SetSystemTimeAdjustment, GetFullPathNameW, FindCloseChangeNotification, SetFileTime, UnlockFile, GetCommandLineW, IsDBCSLeadByteEx, GetTickCount, IsValidLocale, LocalReAlloc
USER32.dll	GetWindowTextLengthW, GetClassLongW, CharNextW, EnumWindows, GetMenuItemCount, GetMenuItemRect, GetKeyboardLayout, CreateDialogParamW, ArrangeIconicWindows, RedrawWindow, GetWindowTextA, ScrollWindowEx, ChildWindowFromPoint, OpenInputDesktop, SetSysColors, SetForegroundWindow, DispatchMessageW, SetCaretPos, ScrollWindow, SendMessageTimeoutA, GetKeyboardLayoutList, DialogBoxParamA, SetScrollInfo, TrackPopupMenuEx, SetWindowTextA, MoveWindow, CascadeWindows, ScreenToClient, CreateDialogParamA, OpenDesktopW, IsRectEmpty, CharUpperBuffA, GetUserObjectInformationA, EnableScrollBar, ShowWindow, SetWindowTextW, MessageBoxExA, CreateCaret, GetClientRect, GetTopWindow, GetSysColorBrush, GetDlgItemInt, GetMenuStringW, GetMessageA, RegisterClassW, LoadMenuA, GetNextDlgGroupItem, wsprintfA, RegisterClassA, ShowOwnedPopups, GetLastActivePopup, SetWindowRgn, CopyImage, DestroyCursor, SetWindowLongW, GetClassInfoExA, GetScrollInfo, FindWindowW, IsCharUpperA, DefDlgProcW, CreateIconFromResource, GetDlgItem, SetDlgItemTextA, CreateWindowExA, GetDlgItemTextW, EnableWindow, LoadIconW, IsWindowUnicode, IsWindowEnabled, IsWindowVisible, IsWindow, AttachThreadInput, GetUserObjectInformationW, GetMessageExtraInfo, CharToOemA, mouse_event, MapVirtualKeyW, SendDlgItemMessageA, InSendMessageEx, GetWindowLongW, GetMessageW, GetParent, DefFrameProcA, SetParent, DestroyWindow, GetMenuItemID, CharToOemBuffA, DispatchMessageA, ShowCaret, GetWindowDC, CharPrevW, PostThreadMessageW, SetDlgItemTextW, LookupIconIdFromDirectory, LockWindowUpdate, GetFocus, ClientToScreen, GrayStringW, SetFocus, TileWindows, ShowScrollBar, CharLowerBuffW, SetMenuDefaultItem, TrackPopupMenu, DeleteMenu, IsCharLowerA, GetCaretPos, ChangeMenuW, SendNotifyMessageW, DialogBoxParamW, CheckRadioButton, SetUserObjectInformationW, SetWindowPlacement, DialogBoxIndirectParamA, InsertMenuW, EnumThreadWindows, SetMenuItemBitmaps, FindWindowExW, MonitorFromRect, GetActiveWindow, SendMessageTimeoutW
MSVCRT.dll	strncpy, wcsncpy, wcsstr, vswprintf, mbtowc, srand, _controlfp, mbstowcs, strcoll, fread, fputc, wcscat, wcstoul, atoi, malloc, __set_app_type, __p__fmode, tolower, strcpy, towlower, ungetc, strpbrk, wcstol, localtime, strstr, wcstombs, __p__commode, _amsg_exit, fflush, puts, _initterm, _ismbblead, wcscpy, strncmp, isupper, _XcptFilter, iswspace, isprint, wcscspn, fgets, _exit, _cexit, __setusermatherr, __getmainargs, strrchr, printf, setlocale

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: citadel_1.3.3.3.exe PID: 5148 Parent PID: 5388

General

Start time:	00:09:00
Start date:	20/07/2020

Path:	C:\Users\user\Desktop\citadel_1.3.3.3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\citadel_1.3.3.3.exe'
Imagebase:	0x400000
File size:	206848 bytes
MD5 hash:	50854EB699ADDE84C0106AC46D7859E5
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: citadel13xy, Description: Citadel 1.5.x.y trojan banker, Source: 00000000.00000002.771080116.0000000000400000.00000040.00020000.sdmp, Author: Jean-Philippe Teissier / @Jipe_
Reputation:	low

Disassembly

Code Analysis