ID: 660113
Sample Name: Rd1Kf1A4cB.bin
Cookbook: default.jbs
Time: 04:01:11
Date: 09/07/2022
Version: 35.0.0 Citrine

Table of Contents

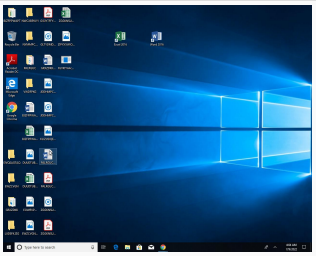
Windows Analysis Report

Rd1Kf1A4cB.bin

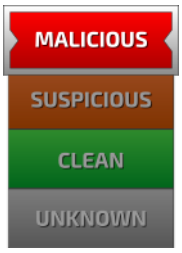
Overview

General Information

Sample Name:	Rd1Kf1A4cB.bin (renamed file extension from bin to exe)
Analysis ID:	660113
MD5:	0ad89e86b34a22.
SHA1:	91a27477c847eb..
SHA256:	f831d088c3a64b..
Tags:	exe zitmo
Infos:	



Detection

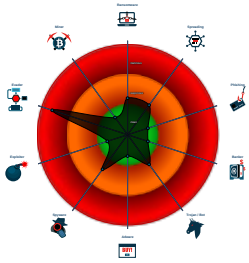


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found evasive API chain (may stop…
- Found evasive API chain (may stop…
- Machine Learning detection for sam…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Extensive use of GetProcAddress (…
- Contains functionality to read the PE…

Classification



Process Tree

- **System is w10x64**
- Rd1Kf1A4cB.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\Rd1Kf1A4cB.exe" MD5: 0AD89E86B34A226FF2A3042103AFC7F1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

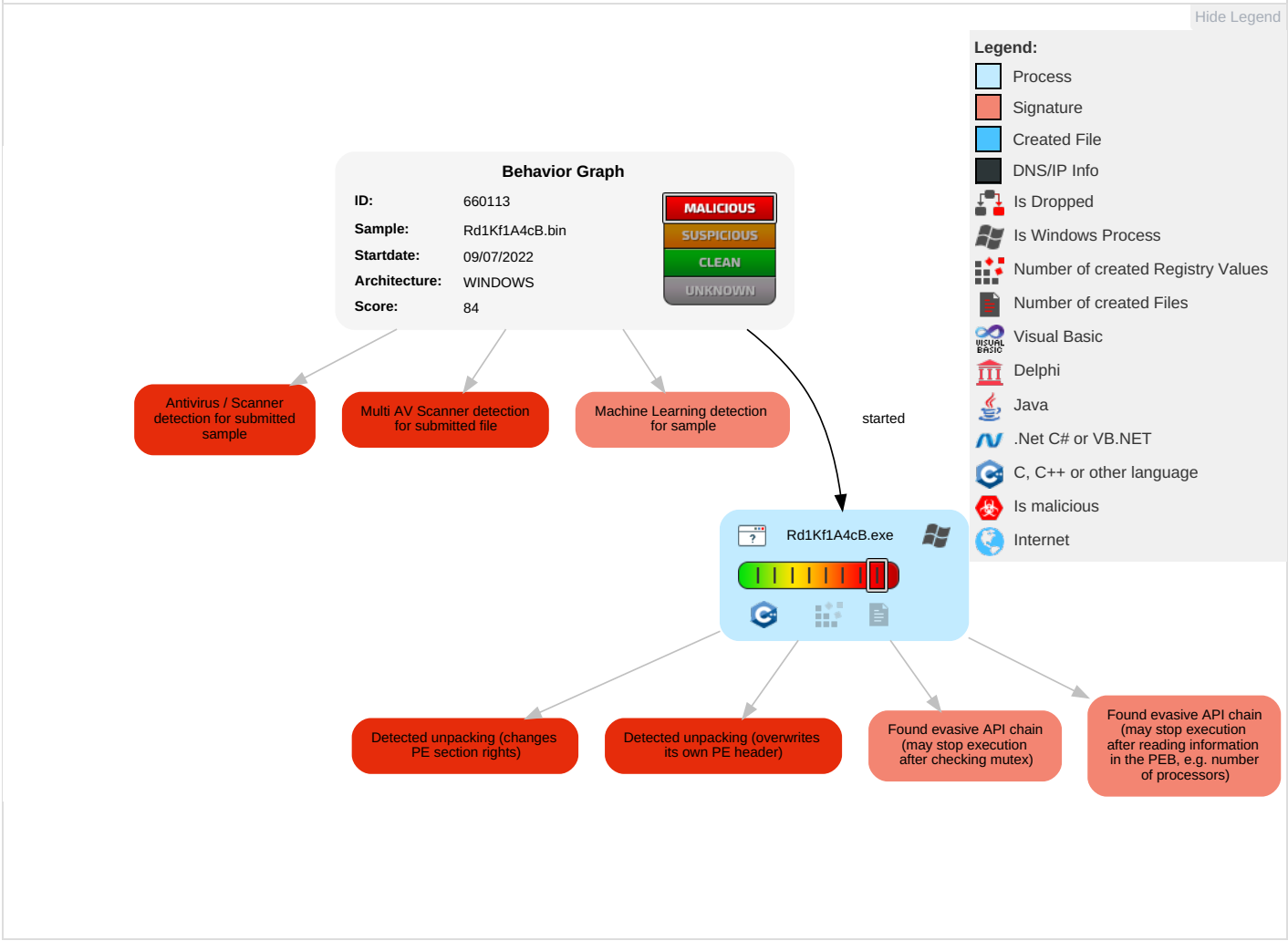
Found evasive API chain (may stop execution after checking mutex)

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
1 Valid Accounts	2 3 Native API	1 Valid Accounts	1 Valid Accounts	1 Valid Accounts	2 1 Input Capture	1 Network Share Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Access Token Manipulation	1 1 Access Token Manipulation	LSASS Memory	2 System Time Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Install Root Certificate	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Clipboard Data	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)	2 1 Software Packing	NTDS	1 Process 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	Software Packing	LSA Secrets	1 Account 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 Owner/User 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	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
Rd1Kf1A4cB.exe	78%	Virustotal		Browse
Rd1Kf1A4cB.exe	96%	ReversingLabs	Win32.Trojan.Zeus	
Rd1Kf1A4cB.exe	100%	Avira	TR/Crypt.XPACK.Gen	
Rd1Kf1A4cB.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Rd1Kf1A4cB.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
0.2.Rd1Kf1A4cB.exe.590000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.Rd1Kf1A4cB.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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://www.google.com/webhpbcsocksGlobal	Rd1Kf1A4cB.exe, 00000000.00000002.260107317.0000000000400000.00000040.00000001.01000000.00000003.sdmp	false		high
http://www.google.com/webhp	Rd1Kf1A4cB.exe, Rd1Kf1A4cB.exe, 00000000.00000002.260107317.0000000000400000.00000040.00000001.01000000.00000003.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	660113
Start date and time: 09/07/202204:01:11	2022-07-09 04:01:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rd1Kf1A4cB.bin (renamed file extension from bin 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:	27
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:	mal84.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.3% (good quality ratio 91.3%) • Quality average: 83.3% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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):	7.50978452876486
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:	Rd1Kf1A4cB.exe
File size:	96256

MD5:	0ad89e86b34a226ff2a3042103afc7f1
SHA1:	91a27477c847ebf9ef3e2cb34e0bc93e323f449d
SHA256:	f831d088c3a64b06843d970337f1c8877c9c1988d56720a7dee9d67efeaf78f0
SHA512:	66149bae72c2c2cff1ce25b03c7f109ab64f8bc80fa22712836bf08843df37cf6e282e4a4776a33bf8c864f0dacb1b928ab44191cb49b65e1c3bad3e53b9d2f4
SSDEEP:	1536:uxDWt8Z1R4ayClVUbHTcM7Y62lO+5FZyoaGSMCDjTyF1ac9OtRHhmV:+Wt8ZIaIVQzccKO+5FqBIItRAV
TLSH:	8693021941C6B4ABEAA44BF71BB5F117302413A14FB246E259A76E3FCF793CE0294349
File Content Preview:	MZ.....@.....|.....!..L.!This program cannot be run in DOS mode....$...PE..L...%..L.....d..... ....@.....dz.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401cd0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NO_SEH
Time Stamp:	0x4CAF0C25 [Fri Oct 8 12:18:45 2010 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:	6ef02dd1adb61f4fee262f301b547fa3

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000002A0h
push ebx
push esi
push edi
push ecx
sub eax, ecx
add dword ptr [ebp-000000B8h], eax

Instruction
sub dword ptr [ebp-000000BBh], eax
mov edi, dword ptr [00402034h]
lea eax, dword ptr [ebp-0Ch]
push eax
mov byte ptr [ebp-0Ch], 00000000h
call edi
xor eax, dword ptr [ebp-1Dh]
mov dword ptr [ebp-1Fh], eax
or dword ptr [ebp-1Fh], eax
mov ebx, dword ptr [0040200Ch]
call ebx
test eax, eax
jne 00007F03A4A2EA54h
call ecx
and dword ptr [ebp-00000171h], eax
and dword ptr [ebp-000001D1h], eax
lea ecx, dword ptr [ebp-6Ch]
push ecx
push FFFFFDF1h
call dword ptr [00402030h]
add esi, dword ptr [ebp-00000220h]
or dword ptr [ebp-0000010Dh], eax
call ebx
test eax, eax
jne 00007F03A4A2EA54h
call esp
or ebx, edi
xor ebx, dword ptr [ebp-00000295h]
push 0000000Fh
push 00000000h
call dword ptr [00402024h]
test eax, eax
jne 00007F03A4A2EA54h
mov edx, dword ptr [edx]
lea edx, dword ptr [ebp-01h]
push edx
mov byte ptr [ebp-01h], 00000000h
call edi
call 00007F03A4A2E14Dh
test eax, eax
je 00007F03A4A2EAA6h
push 00000000h
push 00000000h
push 00000000h
push 00000000h
push 00000000h
push 00000000h
call dword ptr [00402020h]
or ecx, dword ptr [ebp-2Bh]
sub dword ptr [ebp-2Ch], eax
lea eax, dword ptr [ebp-00000268h]
push eax
push FFFFFF23h
call dword ptr [00402030h]
sub edi, dword ptr [ebp+00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17a64	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x280	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2000	0x20	.rdata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2048	0xac	.rdata
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	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	0xe38	0x1000	False	0.58837890625	data	5.938180207293575	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x15c16	0x15e00	False	0.9077901785714285	data	7.598976363385786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x18000	0x6000	0x400	False	0.3388671875	data	3.245150535902098	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x180a0	0x6a	data	English	United States
RT_MANIFEST	0x18110	0x16a	XML 1.0 document, ISO-8859 text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32	GetProcAddress, GetCurrentThread, LoadLibraryA, LocalFree, GetSystemInfo, GetModuleHandleA, CompareStringA, LocalAlloc, CloseHandle
USER32.dll	BeginPaint, CharNextA, DispatchMessageA, GetMessageA, TranslateMessage
ADVAPI32.dll	RegCloseKey

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: Rd1Kf1A4cB.exe PID: 6516, Parent PID: 576

General	
Target ID:	0
Start time:	04:02:18
Start date:	09/07/2022
Path:	C:\Users\user\Desktop\Rd1Kf1A4cB.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Rd1Kf1A4cB.exe"
Imagebase:	0x400000
File size:	96256 bytes
MD5 hash:	0AD89E86B34A226FF2A3042103AFC7F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly