Malware Analysis Report For f409b059205d9a7700d45022dad179f889f18c58c7a284673975271f6af41794

Binary Type

Mach-O (Mach Object). (Approved)

Analyzing File

- **File Name**: f409b059205d9a7700d45022dad179f889f18c58c7a284673975271f6af41794
- **File Extension**: .macho
- **File Type**: Mach-O (Executable)
- **MD5 Hash**: 6d1a07f57da74f474b050228c6422790
- **SHA256 Hash**: f409b059205d9a7700d45022dad179f889f18c58c7a284673975271f6af41794

File Identification

File detected as a valid macOS/iOS executable.

Mach-O File Analysis

Mach-O File Analysis: True

Mach-O File Imports

- CoreFoundation
- CoreGraphics
- Security
- libSystem.B.dylib

Mach-O File Exports

No exported functions were found.

String Analysis

ASCII Strings

- __PAGEZERO
- __TEXT
- __text
- __TEXT
- __stubs
- __TEXT
- _*stub*helper
- __TEXT
- __const
- __TEXT
- __cstring
- __TEXT
- _*unwind*info
- __TEXT
- __DATA
- _*nl*symbol_ptr
- __DATA
- __DATA
- _*la*symbol_ptr
- __DATA
- __const
- __DATA

- __cfstring
- __DATA
- __data
- __DATA
- __common
- __DATA
- __LINKEDIT
- /usr/lib/dyld
- /usr/lib/libSystem.B.dylib
- /System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation
- /System/Library/Frameworks/CoreGraphics.framework/Versions/A/CoreGraphics
- /System/Library/Frameworks/Security.framework/Versions/A/Security
- %)+/5;=CGIOSYaegkmq
- 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz{|
- $%&'()*+,-./0123456789:;<=>?GET /%s HTTP/1.0
- Host: %s
- ERROR: %s
- 1PnYz01rdaiC0000013
- 3iHMvK0RFo0r3KGWvD28URSu06OhV61tdk0t22nizO3nao1q0000033
- 1MNsh21anlz906WugB2zwfjn0000083
- 2D6p7Z0TCrpI0Xr3cd0WnuDn1gwnrz0Tr7f42lQjeq2kmWwq0on0QE1i67sl0zrwpw00exMX3EbFNl3mWoMV10|WBh3HCugK1U|o
- 3lqkFX384jWl2QYw|v0MPF8g2KeKZA3pGX4n0000083
- 05LDJT1j{FSy3Ui0383WYyda0000023
- 0JVurl1WtxB53WxvoP18ouUM2Qo51c3v5dDi0000083
- 2Uy5Dl3hMp7o0cq|T|14vHRz0000013
- 0ZPKhq0rEeUJ0GhPle1joWN30000033
- 0rzACG3Wr||n1dHnZL17MbWe0000013
- 2D6p7Z0TCrpI1Hd1Sr13p2nY2lH{Be2Um4Az1tk62J02KSTK0Kc{CD1icBK92Lsx4E2lywrH1M2tjv1mhaKb0V1vNK2CrQZt1Xn5
- system.privilege.admin
- %s --reroot
- 1nHlTz08Dycj2fGpfB34HNa33yPEb|0NQnSi0j3n3u3JUNmG1uGElB3Rd72B0000033
- --silent
- 2D6p7Z0TCrpI1Hd1Sr13p2nY2lH{Be2Um4Az1tk62J02KSTK0N6aDm1v5klK033Nrh1ecvqP1axrxo3JhSMT2WVZmB2oRkhr1Y7s
- 2D6p7Z0TCrpI1Hd1Sr13p2nY2lH{Be2Um4Az1tk62J02KSTK0N6aDm1v5klK033Nrh1ecvqP1axrxo3JhSMT2WVZmB2oRkhr1Y7s
- 2Y6ndF3HGBhV3OZ5wT2ya9se0000053
- 3mkAT20Khcxt23iYti06y5Ay0000083
- 3mTqdG3tFoV51KYxgy38orxy0000083
- 2Glxas1XPf4|11RXKJ3qj71m0000023
- 3MERln3bPzjJ1bPkcR1QNszj0000023
- 26b0Rr2rjBL52utuBM2otc2K0000083
- 21|sEa0h{uk71aHQBS1jfure0000083
- 0WaAFD1Ltfep3OqVNO0AgDYk0000083
- 0mrCFj3Ek9Uc22CX783oeclT0000083
- 0NpY0y1GYDTG1V2efw1GG2U40000083
- 2GkHc{1m535506JnMW1bv{vW0000043
- 1YhrdL31NSFi37gDFR3WQtHu0000013
- 1DRlzM0o4AeC0UUwhT3F77Wm0000043
- 1YhrdL31NSFi1n5U5l3iQp{L0000013
- 3iJwl71ebaiq0UUwhT3F77Wm0000043
- 1YhrdL31NSFi0vJElt0iGmjl0000013
- 3iJwl71ebaiq3BQAj20QaCZo0000033
- 1YhrdL31NSFi0Lmh{j2aEa6G0LGgHx1hbzVj0000083
- 2l78|i0Wi0rn2YVsFe34WS852c4sUG0lcRl00000083
- 31PjE|0vS2ZW1vAqe72XgFpz1Pl1Yu10DxfT0000023
- _2l78|i0Wi0rn2YVsFe34WS852c4sUG0lcRl00000083
- ei*run*memory_hrd
- /toidievitceffe/libpersist/rennur.c
- junk == 0
- *memory*align
- bufPtr != NULL
- *bufPtr == NULL
- bufSizePtr != NULL
- (err == 0) == (*bufPtr != NULL)
- WorkAroundRadarID4189935
- codeAddrPtr != NULL
- *codeAddrPtr != NULL

- codeSizePtr != NULL
- *codeSizePtr != 0
- ofiPtr != NULL
- *ofiPtr == NULL
- *codeSizePtr* >= *sizeof*(fatHeader)
- fatHeader->magic == FAT_MAGIC
- fatHeader->nfat_arch > 0
- *codeSizePtr* >= *(sizeof*(fatHeader) + (sizeof(*fatArchArray) * fatHeader->nfat_arch))
- ourArch != NULL
- (1 << bestFatArch->align) <= getpagesize()
- bestFatArch->size <= *codeSizePtr
- bestFatArch->offset <= *codeSizePtr
- (bestFatArch->size + bestFatArch->offset) <= *codeSizePtr
- newCodeAddr == NULL
- (dyldErr == NSObjectFileImageSuccess) == (*ofiPtr != NULL)
- %s.%s1
- %s[%s]
- *generate*xkey
- /toidievitceffe/libtpyrc/tpyrc.c
- bits <= 1024
- XY345N5s#p$(:
- ABCDEFGHIJKLMNOPQRSTUVXYZabcdefghijklmnopqrstuvxyz01234567890
- *get*process_list
- /toidievitceffe/libpersist/persist.c
- procList != NULL
- *procList == NULL
- procCount != NULL
- *procList != NULL
- 1bGvlR16wpmp1uNjl83EMxn43AtszK1T6sk02pPg3{3ejPXf1gHmCz313yGx3BrNdJ1oYxn93BET1y09cQl62UVmap1x8Dlx03Jx
- 0hC|h71FgtPJ3oCz{Q3U{4GM0000043
- 0W3iCn1L11zl2H4P|O2xVeOE16|Dem1CSd9k1FZQvS2xelRp3sTLOm0H0pmB0000053
- 0W3iCn1L11zl2H4P|O2xVeOE3sCPHF2EQFF20000063
- 0hC|h71FgtPJ32afft3EzOyU2B0Kih1ww|TZ0000043
- 0hC|h71FgtPJ32afft3EzOyU3xFA7q0{LBxN3vZTtl3quBMg2w77UT0EN8MV0000033
- 1bGvlR16wpmp1uNjl83EMxn43AtszK1T6sk02pPg3{3ejPXf1gHmCz313yGx3BrNdJ1oYxn93BET1y09cQl62UVmap1x8Dlx03Jx
- 1PbP8y2Bxfxk0000013
- 20HBC332gdTh2WTNhS2CgFnL2WBs2l26jxCi0000013
- 0W3iCn1L11zl01EUKl2dH9d{3JeHq507yCvB27MbSd2Yp6dP0000083
- 0hC|h71FgtPJ19|69c0m4GZL1xMqqS3kmZbz3FWvlD1m6d3j0000073
- 3clLm620z4sP2wLtV80WU3qG0000033
- 1utt{h1QSly81vOiy83P9dPz0000013
- q?s=%s&h=%s
- 0Jey2W25rhb50000013
- 2D6p7Z0TCrpl1Hd1Sr13p2nY2lH{Be2Um4Az1tk62J02KSTK2iOZ3l18z1ad36EjC53JE0Vc3dBDxS1eEwU60YbKUZ2enx9z2RQQ
- 1|N|2P1RVDSH0KfURs3Xe2Nd0000073
- .shcsh
- UNDEF:UNDEF:1.3
- %s:%s:1.3
- 1CEMiN3yK6cJ1G8bPi0|Pga00000023
- 1fnh9r02nBQl2shpQT1tVCS10000063
- 0OVBJ303jO5m0000013
- 1CN46O2f8J0d0000023
- 0Q4OMl3kqe|O0000023
- 3dkznH2|EUs906WugB2zwfjn0000083
- 0be|wt12cxKA0SUMNB1EqlJy0000043
- 0QALG60UmDjB3gvZHl1r7tbW0000063
- 20HBC332gdTh2WTNhS2CgFnL3Q0gNf3whEH{0000073
- 0im6vO335|B71Evil505RYE30000023
- 34f3uR1lSUNK1D2bKC2ky9Qr0000023
- 1a7YQt2KJead0000023
- %s --ignrp
- 26aC391KprmW0000013
- --noroot
- --ignrp
- 0XVG|K162Dnf3PNL433RAvye0000053

- 217{Z301RT8X3r7elZ0{99WS0000073
- Cannot create thread!
- This application has to be run by root
- Aborting
- 3epGBa0qgTln00fouX1r8x0T19c6dG0izgBC3NNCQC0NHN5j0qBuWo3ZwmYz2SVos01k51cR1GuWtc3VOjsS3DOZsw0Xig4S1dUZ
- 13roGMpWd7Pb3ZoJyce8eoQpfegQvGHHK7
- 19CMMt3cKbTq0N{VlM35sSlU0DNL6j1U4s6{2sL5ub2qVWlW0000073
- 1BO1|W2SK6rT3ERpNa07rE3z3bN5MA3w1Al32f1U9A1jJemK0mnD2Z0R|eTP00ooBb3sVwBF3{JlME2AuS8u2NcxmC2C0WcD225X
- [decimal]
- [asterisk]
- [plus]
- [clear]
- [divide]
- [enter]
- [hyphen]
- [equals]
- [return]
- [right-cmd]
- [left-cmd]
- [left-shift]
- [caps]
- [left-option]
- [left-ctrl]
- [right-shift]
- [right-option]
- [right-ctrl]
- [volup]
- [voldown]
- [mute]
- [help]
- [home]
- [pgup]
- [fwddel]
- [pgdown]
- [left]
- [right]
- [down]
- [unknown]
- This program is designed to run with admin privileges
- Aborting
- 3lqkFX384jWl1cxKKu1Ypuxw0000043
- 07N{yE26jAdU0000033
- 0VzVyv2CGhca0000033
- 0cYauA1uCR9w0000033
- 36fnal20MdcL0000033
- 0apDeB0bUXYW0000043
- 0KWYxt0liP350000033
- 0bRovT324{db0000043
- 3mfq8Q36s2ss0000033
- 35XC3Y1Wqf450000023
- 2lkRlD07Srpm0000033
- 3JK6CK3AfpfK0000033
- 0BJAms2p4jOj0000033
- 2SgYG41upIVv0000033
- 2WRrXd2EylAS0000033
- 37Ruu706Dlx80000033
- 1c51023qApwy0000033
- 3SSsC02VYt9v0000033
- 1GDUmR18twt00000033
- 148g9G0h2eiz0000033
- 3jHqjH2L7YxN0000033
- 08xZTy3z8MpB0000023
- 2TgstP2|ZKMd0000033
- 3Es0yh0GAW|k0000023
- 0nM0qd30jrYq0000033
- 33eTui0d8Opa0000033

- 1OVloe30NkdI0000023
- 1|s3Z{3ieBzL0000033
- 0zDja000HFM70000023
- 2QdWaA23sONd0000013
- 0Mj2nC25XyAW0000033
- 2yUBhg0qFRrx0000033
- 1fh6J23Qe|sY0000033
- 2v252Q2nRRRT0000033
- 2b08VH0C3VLJ0000023
- 0p3Oya2LzKFY0000023
- 2ZgQGK1qRReE0000033
- 0LP48z2DqlgK0000033
- 3eR2Cf0yU6RM0000033
- 0DG1f93Nclal0000053
- 3wbf6m0vv0lD0000033
- 0Qz|0E0k1pPA0000053
- 1CUrTd1L{gP90000053
- 2|RsdH38O0CU0000033
- 2dZ9FU3VB1lx0000033
- 0WYJfP3RA1Z90000033
- 07|iMc1yBLAf0000023
- 2aFLuH2QgXyZ0000023
- 2bst191PereF0000033
- 13RXRH0sQey50000033
- 25BFu33ldq{Y0000033
- 0j9D{60zzQJz0000043
- 2N00Qj3pZfW20000043
- 1JtccJ1KczPw0000033
- 3Cfh7Y2dET2a0000033
- 1VH2YK2ESC6l0000033
- 3az9GJ2JxCer0000043
- 1xJrSy1pXbRF0000033
- 0Lk8Li3fOjd20000033
- 1YqHpV0SCvBp0000033
- 0iDLz{2XaJdD0000033
- 2BXjr41H0Lgc0000023
- 2dsbkh0yNuly3RvUBd3N{RiA0000063
- 1pvJkl3SfoRF0000033
- 3cpv7p3MSRg111WV3e0Cxekc0000073
- 0dvNvQ1ehl3q1Re5xU2ODLy90000073
- 20ZmmJ3|T5WT0000033
- 1qHMll1PIV{l0000023
- 1Jj06r29W{ot0000023
- 3guFUf2WlEUl0000033
- 37FWof0D0MeL0000023
- 1ONkV80vfbhT0000043
- 1Vzmwo3iAfRL3Tssx21oG17t0000083
- 0vOxwn02kLKr0000023
- 34rROO1bjXLX0000033
- 3vhJwh2yDEo|19bBKE3UVNA30000043
- "0 `\D`
- `LBpH\
- @_stack*chk*guard
- @*mach*task*self*
- @dyld*stub*binder
- @_CFConstantStringClassReference
- @_kCFAllocatorDefault
- @_kCFRunLoopCommonModes
- @_AuthorizationCopyRights
- @_AuthorizationCreate
- @_CFBundleCreate
- @_CFBundleGetFunctionPointerForName
- @_CFMachPortCreateRunLoopSource
- @_CFRelease
- @_CFRunLoopAddSource
- @_CFRunLoopGetCurrent

- @_CFRunLoopRun
- @_CFURLCreateFromFileSystemRepresentation
- @_CGEventGetIntegerValueField
- @_CGEventTapCreate
- @_CGEventTapEnable
- @_NSAddressOfSymbol
- @_NSCreateObjectFileImageFromMemory
- @_NSDestroyObjectFileImage
- @_NSLinkModule
- @_NSLookupSymbolInModule
- @_NSUnLinkModule
- @_NXFindBestFatArch
- @_NXGetLocalArchInfo
- @_assert_rtn
- @_error
- @_memcpy_chk
- @_memset_chk
- @_sprintf_chk
- @_stack*chk*fail
- @_calloc
- @_chmod
- @_close
- @_closedir
- @_connect
- @_execl
- @_execv
- @_exit
- @_fclose
- @_fopen
- @_fork
- @_fread
- @_free
- @_fseek
- @_ftell
- @_ftrylockfile
- @_funlockfile
- @_fwrite
- @_getenv
- @_geteuid
- @_gethostbyname
- @_gethostname
- @_getlogin
- @_getpagesize
- @_getpid
- @*if*nametoindex
- @_kevent
- @_kill
- @_kqueue
- @_malloc
- @_memcpy
- @_memset
- @_mkdir
- @*nl*langinfo
- @_open
- @_opendir$INODE64
- @_popen
- @_printf
- @*pthread*create
- @_ptrace
- @_random
- @_read
- @_readdir$INODE64
- @_realloc
- @_rename
- @_sleep

- @_socket
- @_srandom
- @_stat$INODE64
- @_strcasestr
- @_strcmp
- @_strerror
- @_strlen
- @_strrchr
- @_strstr
- @_sysctl
- @_system
- @_time
- @_uname
- @_unlink
- @*vm*allocate
- @*vm*deallocate
- @_write
- http_request
- pack_trailer
- unpack_trailer
- home_stub
- dispatch
- is_target
- h*execute*header
- ake*temp*name
- lf*rglk*watch_routine
- forensic_
- loader_
- carver_main
- ave_spot
- elfretain_main
- _encode
- serialize_request
- deserialize_request
- make_request
- sendfile
- thread
- ead_spot
- ootgainer_main
- show_alert
- communicate
- launch_helper
- ave_message
- ignature
- h*cmd*async
- andom_key
- as_admin
- regular
- daemon
- target
- _async
- cquire_root
- ppend_ei
- _async
- onstruct*plist*path
- heck*if*targeted
- ser_info
- rlsafe
- ncarve_target
- nstall_daemon
- lfsc_target
- executable
- debugging
- virtual_mchn
- carved

- file_target
- dirlist
- get_contents
- unpack_binary
- ck_binary
- rse_template
- memory_hrd
- thread
- ract_ei
- ended*check*modification
- yncsem
- random_action
- save_spot
- get_spot
- is*high*time
- carve*or*not
- append*or*not
- pyrc_checksum
- host_info
- macaddr
- nerate_xkey
- encrypt
- decrypt
- dcrypt
- reate*rescue*executable
- arve_target
- if_running
- modification
- file_exists
- encrypt
- decrypt
- ersist_executable
- event_trace
- ocess_event
- iv*rescue*data
- process_list
- host_identifier
- ill_unwanted
- convert
- uild_plist
- resque_data
- important_files
- sque_myself
- lease_events
- _frombundle
- _thread
- istence_main
- init*crc32*tab
- rootgainer_elevate
- mediator
- targets
- check_command
- append_command
- drop_ccache
- get_update
- thread
- ediated
- pack_c
- unpack_i
- encode
- decode
- ecure_
- tring_
- encode
- decode

- UNWANTED
- SELFNAMES
- INSTSGN
- RESCUE
- askroot
- failed_asks
- __PAGEZERO
- __TEXT
- __text
- __TEXT
- __stubs
- __TEXT
- _*stub*helper
- __TEXT
- __const
- __TEXT
- __cstring
- __TEXT
- _*unwind*info
- __TEXT
- __DATA
- _*nl*symbol_ptr
- __DATA
- __DATA
- _*la*symbol_ptr
- __DATA
- __const
- __DATA
- __cfstring
- __DATA
- __data
- __DATA
- __common
- __DATA
- __LINKEDIT
- /usr/lib/dyld
- /usr/lib/libSystem.B.dylib
- /System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation
- /System/Library/Frameworks/CoreGraphics.framework/Versions/A/CoreGraphics
- /System/Library/Frameworks/Security.framework/Versions/A/Security
- "0 `\D`
- `LBpH\
- @_stack*chk*guard
- @*mach*task*self*
- @dyld*stub*binder
- @_CFConstantStringClassReference
- @_kCFAllocatorDefault
- @_kCFRunLoopCommonModes
- @_AuthorizationCopyRights
- @_AuthorizationCreate
- @_CFBundleCreate
- @_CFBundleGetFunctionPointerForName
- @_CFMachPortCreateRunLoopSource
- @_CFRelease
- @_CFRunLoopAddSource
- @_CFRunLoopGetCurrent
- @_CFRunLoopRun
- @_CFURLCreateFromFileSystemRepresentation
- @_CGEventGetIntegerValueField
- @_CGEventTapCreate
- @_CGEventTapEnable
- @_NSAddressOfSymbol
- @_NSCreateObjectFileImageFromMemory
- @_NSDestroyObjectFileImage
- @_NSLinkModule

- @_NSLookupSymbolInModule
- @_NSUnLinkModule
- @_NXFindBestFatArch
- @_NXGetLocalArchInfo
- @_assert_rtn
- @_error
- @_memcpy_chk
- @_memset_chk
- @_sprintf_chk
- @_stack*chk*fail
- @_calloc
- @_chmod
- @_close
- @_closedir
- @_connect
- @_execl
- @_execv
- @_exit
- @_fclose
- @_fopen
- @_fork
- @_fread

UTF-8 Strings

No detected.

UTF-16LE Strings

- 3asdfhgzxcvbqeyt123465=97-80]ou[iplj'k;\,/nm`

Extracted URLs

No detected.

Base64 Strings

No valid Base64-encoded strings found.

File Entropy Analysis

- **Entropy**: `5.75`
- **Status**: This file likely contains Standard Text or human-readable text.

VirusTotal Analysis

Scan Date: 2025-02-07 23:08:56

Scan Results

- Malicious: 42
- Suspicious: 0
- Undetected: 20
- Harmless: 0
- Timeout: 0
- Confirmed-timeout: 0
- Failure: 0
- Type-unsupported: 13

Community Votes

- Harmless: 0
- Malicious: 5

Detailed Engine Results

Engine Name	Detection Category	Detection
Lionic	malicious	Virus.OSX.MacRansom.n!c
Elastic	malicious	malicious (high confidence)
Cynet	malicious	Malicious (score: 99)
Skyhigh	malicious	OSX/VirRansom.a
ALYac	malicious	Trojan.Ransom.OSX.MacRansom
Zillya	malicious	Trojan.Filecoder.OSX.5
K7GW	malicious	Trojan (3ac070911)
Arcabit	malicious	Trojan.MAC.MacRansom.K
huorong	malicious	Ransom/OSX.EvilQuest.b
Symantec	malicious	OSX.RansomThiefQuest
ESET-NOD32	malicious	OSX/Filecoder.EvilQuest.A
TrendMicro-HouseCall	malicious	Ransom.MacOS.EVILQUEST.A
Avast	malicious	MacOS:Filecoder-J [Trj]
ClamAV	malicious	Osx.Ransomware.ThiefQuest-8825524-0
Kaspersky	malicious	Virus.OSX.ThifQseut.a
BitDefender	malicious	Trojan.MAC.MacRansom.K
ViRobot	malicious	Trojan.OSX.S.Agent.98304
MicroWorld-eScan	malicious	Trojan.MAC.MacRansom.K
Tencent	malicious	Osx.Virus.Thifqseut.Mcnw
Emsisoft	malicious	Trojan.MAC.MacRansom.K (B)
F-Secure	malicious	Malware.OSX/Filecoder.O
DrWeb	malicious	Mac.Encoder.5
VIPRE	malicious	Trojan.MAC.MacRansom.K
TrendMicro	malicious	Ransom.MacOS.EVILQUEST.A
CTX	malicious	macho.ransomware.filecoder
Sophos	malicious	OSX/Filecode-S
Ikarus	malicious	OSX.Agent
FireEye	malicious	Trojan.MAC.MacRansom.K
Avira	malicious	OSX/Filecoder.O
Xcitium	malicious	Malware@#218nr8pwq9k63
Microsoft	malicious	Ransom:MacOS/Filecoder.YA!MTB
GData	malicious	Trojan.MAC.MacRansom.K
Varist	malicious	MacOS/MacRansom5.A
AhnLab-V3	malicious	Trojan/OSX.Ransom.98304
McAfee	malicious	OSX/VirRansom.a
Rising	malicious	Ransom.EvilQuest/OSX!1.D95D (CLASSIC)
SentinelOne	malicious	Static AI - Malicious Mach-O
MaxSecure	malicious	Virus.Mac.Ransomwre.ci
Fortinet	malicious	MAC/Filecode.S!tr.ransom
AVG	malicious	MacOS:Filecoder-J [Trj]
alibabacloud	malicious	Ransomware:MacOS/EvilQuest.A