VALKYRIE COMODO

Summary

File Name: advanced-rar-repair-programas-gratis-net.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

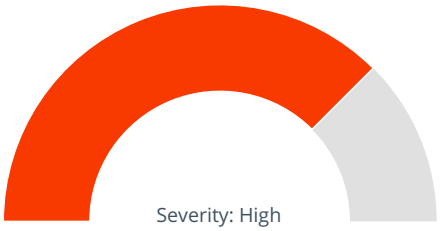
SHA1: 55bfa6aa04a16a892acdb2cc410192ab21e886a3

MD5: 178b4faf2ee615e96d2b27d0cd94794b

MALWARE

Valkyrie Final Verdict

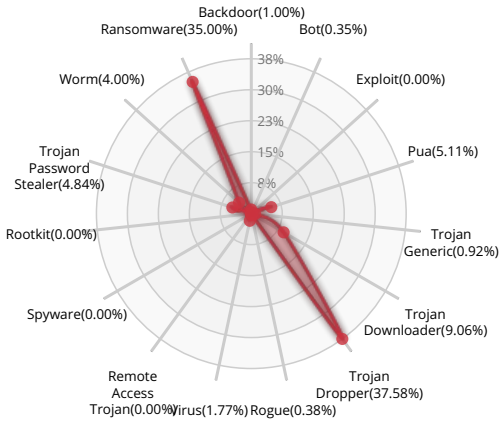
DETECTION SECTION



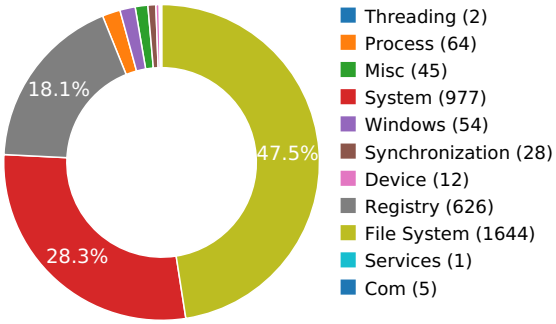
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Exhibits possible ransomware file modification behavior — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

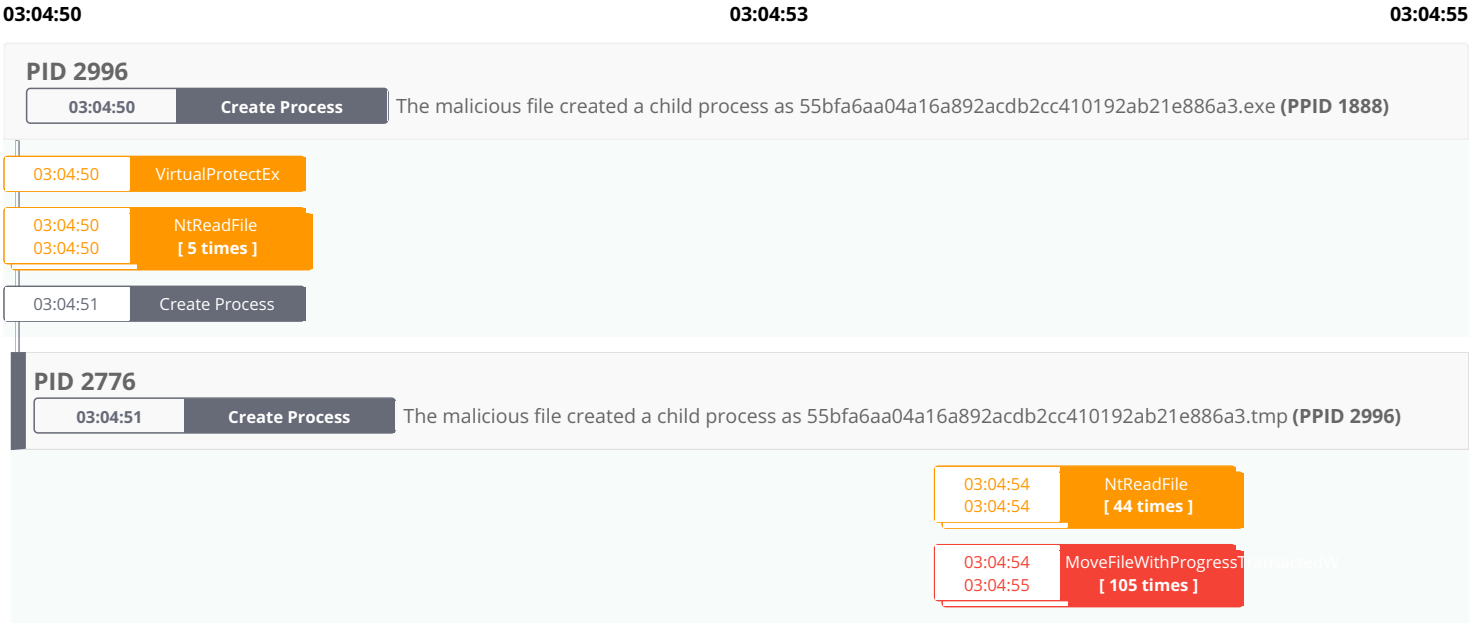
Creates RWX memory

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_shfoldr.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
c:\directory
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\
C:\Program Files (x86)\Hohi\
C:\Program Files (x86)\
C:\Program Files (x86)\Hohi
C:\Program Files (x86)\Hohi\Fokufofefo.exe
C:\Program Files (x86)\Hohi\Funagub.exe
C:\Program Files (x86)\Hohi\Lefag.exe
C:\Program Files (x86)\Hohi\Rokicaha.exe
C:\Windows\System32
C:\Program Files (x86)

C:\Program Files (x86)\Hohi\unins???.*

C:\Program Files (x86)\Hohi\unins000.dat

C:\Windows\winsxs\FileMaps\program_files_x86_hohi_32386b0764e70aa0.cdf-ms

C:\Program Files (x86)\Hohi\unins000.exe

C:\Program Files (x86)\Hohi\is-R6K87.tmp

C:\Program Files (x86)\Hohi\Rukunododor.odt

C:\Program Files (x86)\Hohi\is-VR1V2.tmp

C:\Program Files (x86)\Hohi\Dilebenet.h

C:\Program Files (x86)\Hohi\is-9UTHG.tmp

C:\Program Files (x86)\Hohi\Lepim.ke

C:\Program Files (x86)\Hohi\is-MF2ET.tmp

C:\Program Files (x86)\Hohi\Logacodol.com

C:\Program Files (x86)\Hohi\is-6PA85.tmp

C:\Program Files (x86)\Hohi\Dusotedam.html

C:\Program Files (x86)\Hohi\is-AQ55P.tmp

C:\Program Files (x86)\Hohi\Decodusehupi.log

C:\Program Files (x86)\Hohi\is-29NM3.tmp

C:\Program Files (x86)\Hohi\Pamakomab.cumi

C:\Program Files (x86)\Hohi\is-KKNKU.tmp

C:\Program Files (x86)\Hohi\Kelanu.pptx

C:\Program Files (x86)\Hohi\is-5IGHC.tmp

C:\Program Files (x86)\Hohi\Caluselah.mpg

C:\Program Files (x86)\Hohi\is-3JIAR.tmp

C:\Program Files (x86)\Hohi\Tusepof.wpd

C:\Program Files (x86)\Hohi\is-D8U2B.tmp

C:\Program Files (x86)\Hohi\Ciberalina.html

C:\Program Files (x86)\Hohi\is-U4EH6.tmp

C:\Program Files (x86)\Hohi\Cikasipo.vob

C:\Program Files (x86)\Hohi\is-O2LPJ.tmp

C:\Program Files (x86)\Hohi\Dacafola.pptx

C:\Program Files (x86)\Hohi\is-D7AQV.tmp

C:\Program Files (x86)\Hohi\Lireta.csv

C:\Program Files (x86)\Hohi\is-K1FM0.tmp

C:\Program Files (x86)\Hohi\Hupanane.odt

C:\Program Files (x86)\Hohi\is-REQ2C.tmp

C:\Program Files (x86)\Hohi\Rabarop.html
C:\Program Files (x86)\Hohi\is-6JGQJ.tmp
C:\Program Files (x86)\Hohi\Puritocon.ppt
C:\Program Files (x86)\Hohi\is-TNOMT.tmp
C:\Program Files (x86)\Hohi\is-RNMKP.tmp
C:\Program Files (x86)\Hohi\Noheninened.bega
C:\Program Files (x86)\Hohi\is-G54R9.tmp
C:\Program Files (x86)\Hohi\Linegori.sdf
C:\Program Files (x86)\Hohi\is-C6EI3.tmp

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\D06EB8C2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations2
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0001
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegSvcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegProcs0000
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\unins000.exe

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Rukunododor.odt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Dilebenet.h
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Lepim.ke
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Logacodol.com
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Dusotedam.html
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Decodusehupi.log
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Pamakomab.cumi
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Kelanu.pptx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Caluselah.mpg
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Tusepof.wpd
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Ciberalina.html
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Cikasipo.vob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Dacafola.pptx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Lireta.csv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Hupanane.odt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Rabarop.html
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Puritocon.ppt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Hohi\Funagub.exe

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_shfoldr.dll
C:\Program Files (x86)\Hohi\Fokufofefo.exe
C:\Program Files (x86)\Hohi\Funagub.exe
C:\Program Files (x86)\Hohi\Lefag.exe
C:\Program Files (x86)\Hohi\Rokicaha.exe
C:\Program Files (x86)\Hohi\unins000.dat
C:\Program Files (x86)\Hohi\is-R6K87.tmp
C:\Program Files (x86)\Hohi\unins000.exe
C:\Program Files (x86)\Hohi\is-VR1V2.tmp
C:\Program Files (x86)\Hohi\Rukunododor.odt
C:\Program Files (x86)\Hohi\is-9UTHG.tmp
C:\Program Files (x86)\Hohi\Dilebenet.h
C:\Program Files (x86)\Hohi\is-MF2ET.tmp

C:\Program Files (x86)\Hohi\Lepim.ke
C:\Program Files (x86)\Hohi\is-6PA85.tmp
C:\Program Files (x86)\Hohi\Logacodol.com
C:\Program Files (x86)\Hohi\is-AQ55P.tmp
C:\Program Files (x86)\Hohi\Dusotedam.html
C:\Program Files (x86)\Hohi\is-29NM3.tmp
C:\Program Files (x86)\Hohi\Decodusehupi.log
C:\Program Files (x86)\Hohi\is-KKNKU.tmp
C:\Program Files (x86)\Hohi\Pamakomab.cumi
C:\Program Files (x86)\Hohi\is-5IGHC.tmp
C:\Program Files (x86)\Hohi\Kelanu.pptx
C:\Program Files (x86)\Hohi\is-3JIAR.tmp
C:\Program Files (x86)\Hohi\Caluselah.mpg
C:\Program Files (x86)\Hohi\is-D8U2B.tmp
C:\Program Files (x86)\Hohi\Tusepof.wpd
C:\Program Files (x86)\Hohi\is-U4EH6.tmp
C:\Program Files (x86)\Hohi\Ciberalina.html
C:\Program Files (x86)\Hohi\is-O2LPJ.tmp
C:\Program Files (x86)\Hohi\Cikasipo.vob
C:\Program Files (x86)\Hohi\is-D7AQV.tmp
C:\Program Files (x86)\Hohi\Dacafola.pptx
C:\Program Files (x86)\Hohi\is-K1FM0.tmp
C:\Program Files (x86)\Hohi\Lireta.csv
C:\Program Files (x86)\Hohi\is-REQ2C.tmp
C:\Program Files (x86)\Hohi\Hupanane.odt
C:\Program Files (x86)\Hohi\is-6JGQJ.tmp
C:\Program Files (x86)\Hohi\Rabarop.html
C:\Program Files (x86)\Hohi\is-TNOMT.tmp
C:\Program Files (x86)\Hohi\Puritocon.ppt
C:\Program Files (x86)\Hohi\is-RNMKP.tmp
C:\Program Files (x86)\Hohi\is-G54R9.tmp
C:\Program Files (x86)\Hohi\Noheninened.bega
C:\Program Files (x86)\Hohi\is-C6EI3.tmp
C:\Program Files (x86)\Hohi\Linegori.sdf
C:\Program Files (x86)\Hohi\is-31KJE.tmp

C:\Program Files (x86)\Hohi\Fasedoc.hi
C:\Program Files (x86)\Hohi\is-3866E.tmp
C:\Program Files (x86)\Hohi\Rolamuga.fat
C:\Program Files (x86)\Hohi\is-DM72K.tmp
C:\Program Files (x86)\Hohi\Dubepekadi.jar
C:\Program Files (x86)\Hohi\is-B401S.tmp
C:\Program Files (x86)\Hohi\Secafota.sdf
C:\Program Files (x86)\Hohi\is-N9BPA.tmp
C:\Program Files (x86)\Hohi\Fusab.rtf
C:\Program Files (x86)\Hohi\is-F9OMO.tmp
C:\Program Files (x86)\Hohi\Latupubap.cpp
C:\Program Files (x86)\Hohi\is-DNSJ6.tmp
C:\Program Files (x86)\Hohi\Tolub.csv
C:\Program Files (x86)\Hohi\is-6C8FL.tmp
C:\Program Files (x86)\Hohi\Sasetef.vob
C:\Program Files (x86)\Hohi\is-ED658.tmp
C:\Program Files (x86)\Hohi\Siracatusem.nesi
C:\Program Files (x86)\Hohi\is-K8DLF.tmp
C:\Program Files (x86)\Hohi\Pogalerehe.bat
C:\Program Files (x86)\Hohi\is-1DQRN.tmp
C:\Program Files (x86)\Hohi\is-3OB57.tmp
C:\Program Files (x86)\Hohi\Keber.mp3
C:\Program Files (x86)\Hohi\is-ECC81.tmp
C:\Program Files (x86)\Hohi\Pegusogam.m3u
C:\Program Files (x86)\Hohi\is-L97M9.tmp
C:\Program Files (x86)\Hohi\Cecudagede.log

RESOLVED APIS

kernel32.dll.SetDllDirectoryW
kernel32.dll.SetSearchPathMode
kernel32.dll.SetProcessDEPPolicy
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.GetModuleFileNameW

kernel32.dll.CreateFileW
kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.FreeLibrary
kernel32.dll.DeleteCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.InitializeCriticalSection
kernel32.dll.LocalFree
kernel32.dll.LocalAlloc
kernel32.dll.GetCurrentThreadId
kernel32.dll.WideCharToMultiByte
kernel32.dll.lstrlenA
kernel32.dll.lstrcpynA
kernel32.dll.LoadLibraryExA
kernel32.dll.GetThreadLocale
kernel32.dll.GetStartupInfoA
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetCommandLineA
kernel32.dll.FindFirstFileA
kernel32.dll.FindClose
kernel32.dll.ExitProcess
kernel32.dll.WriteFile
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.RtlUnwind
kernel32.dll.RaiseException
kernel32.dll.GetStdHandle
user32.dll.GetKeyboardType
user32.dll.LoadStringA
user32.dll.MessageBoxA

user32.dll.CharNextA
advapi32.dll.RegQueryValueExA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegCloseKey
oleaut32.dll.SysFreeString
oleaut32.dll.SysReAllocStringLen
kernel32.dll.TlsSetValue
kernel32.dll.TlsGetValue
kernel32.dll.TlsFree
kernel32.dll.TlsAlloc
kernel32.dll.VirtualQueryEx
kernel32.dll.VirtualQuery
kernel32.dll.SetConsoleTextAttribute
kernel32.dll.ReadProcessMemory
kernel32.dll.OpenProcess
kernel32.dll.MoveFileExA
kernel32.dll.MapViewOfFileEx
kernel32.dll.GetVersionExA
kernel32.dll.GetTickCount
kernel32.dll.GetSystemInfo
kernel32.dll.GetStringTypeExA
kernel32.dll.GetProfileIntA
kernel32.dll.GetDiskFreeSpaceA
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCPInfo
kernel32.dll.GetACP
kernel32.dll.EnumCalendarInfoA
kernel32.dll.CloseHandle
user32.dll.IsDlgButtonChecked
user32.dll.HiliteMenuItem
user32.dll.GetSystemMetrics
user32.dll.GetLastInputInfo
user32.dll.DialogBoxParamA
user32.dll.DeferWindowPos

DELETED FILES

C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp
C:\Program Files (x86)\Hohi\is-R6K87.tmp
C:\Program Files (x86)\Hohi\is-VR1V2.tmp
C:\Program Files (x86)\Hohi\is-9UTHG.tmp
C:\Program Files (x86)\Hohi\is-MF2ET.tmp
C:\Program Files (x86)\Hohi\is-6PA85.tmp
C:\Program Files (x86)\Hohi\is-AQ55P.tmp
C:\Program Files (x86)\Hohi\is-29NM3.tmp
C:\Program Files (x86)\Hohi\is-KKNKU.tmp
C:\Program Files (x86)\Hohi\is-5IGHC.tmp
C:\Program Files (x86)\Hohi\is-3JIAR.tmp
C:\Program Files (x86)\Hohi\is-D8U2B.tmp
C:\Program Files (x86)\Hohi\is-U4EH6.tmp
C:\Program Files (x86)\Hohi\is-O2LPJ.tmp
C:\Program Files (x86)\Hohi\is-D7AQV.tmp
C:\Program Files (x86)\Hohi\is-K1FM0.tmp
C:\Program Files (x86)\Hohi\is-REQ2C.tmp
C:\Program Files (x86)\Hohi\is-6JGQJ.tmp
C:\Program Files (x86)\Hohi\is-TNOMT.tmp
C:\Program Files (x86)\Hohi\is-RNMKP.tmp
C:\Program Files (x86)\Hohi\is-G54R9.tmp
C:\Program Files (x86)\Hohi\is-C6EI3.tmp
C:\Program Files (x86)\Hohi\is-31KJE.tmp
C:\Program Files (x86)\Hohi\is-3866E.tmp
C:\Program Files (x86)\Hohi\is-DM72K.tmp
C:\Program Files (x86)\Hohi\is-B401S.tmp
C:\Program Files (x86)\Hohi\is-N9BPA.tmp
C:\Program Files (x86)\Hohi\is-F9OMO.tmp
C:\Program Files (x86)\Hohi\is-DNSJ6.tmp
C:\Program Files (x86)\Hohi\is-6C8FL.tmp
C:\Program Files (x86)\Hohi\is-ED658.tmp
C:\Program Files (x86)\Hohi\is-K8DLF.tmp
C:\Program Files (x86)\Hohi\is-1DQRN.tmp

C:\Program Files (x86)\Hohi\is-3OB57.tmp

C:\Program Files (x86)\Hohi\is-ECC81.tmp

C:\Program Files (x86)\Hohi\is-L97M9.tmp

C:\Program Files (x86)\Hohi\is-AT6UT.tmp

C:\Program Files (x86)\Hohi\is-1SPG9.tmp

C:\Program Files (x86)\Hohi\is-BJD6C.tmp

C:\Program Files (x86)\Hohi\is-O7AH1.tmp

C:\Program Files (x86)\Hohi\is-UTBJJ.tmp

C:\Program Files (x86)\Hohi\is-LT12K.tmp

C:\Program Files (x86)\Hohi\is-AT4P1.tmp

C:\Program Files (x86)\Hohi\is-LPP1D.tmp

C:\Program Files (x86)\Hohi\is-JLF4F.tmp

C:\Program Files (x86)\Hohi\is-BVPHV.tmp

C:\Program Files (x86)\Hohi\is-IP1CP.tmp

C:\Program Files (x86)\Hohi\is-LIJ75.tmp

C:\Program Files (x86)\Hohi\is-AN9G9.tmp

C:\Program Files (x86)\Hohi\is-EKIO3.tmp

C:\Program Files (x86)\Hohi\is-T6A2C.tmp

C:\Program Files (x86)\Hohi\is-D6K62.tmp

C:\Program Files (x86)\Hohi\is-B6Q9Q.tmp

C:\Program Files (x86)\Hohi\is-VQ2IN.tmp

C:\Program Files (x86)\Hohi\is-3K4EH.tmp

C:\Program Files (x86)\Hohi\is-2EG5S.tmp

C:\Program Files (x86)\Hohi\is-9UUNP.tmp

C:\Program Files (x86)\Hohi\is-NLJ3K.tmp

C:\Program Files (x86)\Hohi\is-6MQQ1.tmp

C:\Program Files (x86)\Hohi\is-NGIIA.tmp

C:\Program Files (x86)\Hohi\is-537KV.tmp

C:\Program Files (x86)\Hohi\is-4BGGH.tmp

C:\Program Files (x86)\Hohi\is-R221J.tmp

C:\Program Files (x86)\Hohi\is-H3RR4.tmp

C:\Program Files (x86)\Hohi\is-0EFG3.tmp

C:\Program Files (x86)\Hohi\is-E8N37.tmp

C:\Program Files (x86)\Hohi\is-CNVLV.tmp

C:\Program Files (x86)\Hohi\is-DRVK3.tmp

C:\Program Files (x86)\Hohi\is-OEGBU.tmp
C:\Program Files (x86)\Hohi\is-CD19D.tmp
C:\Program Files (x86)\Hohi\is-ITFRV.tmp
C:\Program Files (x86)\Hohi\is-EE2KV.tmp
C:\Program Files (x86)\Hohi\is-8SPV8.tmp
C:\Program Files (x86)\Hohi\is-S6LKS.tmp
C:\Program Files (x86)\Hohi\is-L3BC8.tmp

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\D06EB8C2
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Sans Serif
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Verdana
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software
HKEY_LOCAL_MACHINE\Software
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-53TKA.tmp_isetup_shfoldr.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll

C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\
C:\Program Files (x86)\Hohi\Fokufofefo.exe
C:\Program Files (x86)\Hohi\Funagub.exe
C:\Program Files (x86)\Hohi\Lefag.exe
C:\Program Files (x86)\Hohi\Rokicaha.exe
C:\Program Files (x86)\Hohi\unins000.dat
C:\Windows\winsxs\FileMaps\program_files_x86_hohi_32386b0764e70aa0.cdf-ms
C:\Program Files (x86)\Hohi\is-R6K87.tmp
C:\Users\user\AppData\Local\Temp\is-L8P07.tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.tmp
C:\Program Files (x86)\Hohi\is-VR1V2.tmp
C:\Program Files (x86)\Hohi\is-9UTHG.tmp
C:\Program Files (x86)\Hohi\is-MF2ET.tmp
C:\Program Files (x86)\Hohi\is-6PA85.tmp
C:\Program Files (x86)\Hohi\is-AQ55P.tmp
C:\Program Files (x86)\Hohi\is-29NM3.tmp
C:\Program Files (x86)\Hohi\is-KKNKU.tmp
C:\Program Files (x86)\Hohi\is-5IGHC.tmp
C:\Program Files (x86)\Hohi\is-3JIAR.tmp
C:\Program Files (x86)\Hohi\is-D8U2B.tmp
C:\Program Files (x86)\Hohi\is-U4EH6.tmp
C:\Program Files (x86)\Hohi\is-O2LPJ.tmp
C:\Program Files (x86)\Hohi\is-D7AQV.tmp
C:\Program Files (x86)\Hohi\is-K1FM0.tmp
C:\Program Files (x86)\Hohi\is-REQ2C.tmp
C:\Program Files (x86)\Hohi\is-6JGQJ.tmp
C:\Program Files (x86)\Hohi\is-TNOMT.tmp
C:\Program Files (x86)\Hohi\is-RNMKP.tmp
C:\Program Files (x86)\Hohi\is-G54R9.tmp
C:\Program Files (x86)\Hohi\is-C6EI3.tmp
C:\Program Files (x86)\Hohi\is-31KJE.tmp
C:\Program Files (x86)\Hohi\is-3866E.tmp
C:\Program Files (x86)\Hohi\is-DM72K.tmp
C:\Program Files (x86)\Hohi\is-B401S.tmp

C:\Program Files (x86)\Hohi\is-N9BPA.tmp
C:\Program Files (x86)\Hohi\is-F9OMO.tmp
C:\Program Files (x86)\Hohi\is-DNSJ6.tmp
C:\Program Files (x86)\Hohi\is-6C8FL.tmp
C:\Program Files (x86)\Hohi\is-ED658.tmp
C:\Program Files (x86)\Hohi\is-K8DLF.tmp
C:\Program Files (x86)\Hohi\is-1DQRN.tmp
C:\Program Files (x86)\Hohi\is-3OB57.tmp
C:\Program Files (x86)\Hohi\is-ECC81.tmp
C:\Program Files (x86)\Hohi\is-L97M9.tmp
C:\Program Files (x86)\Hohi\is-AT6UT.tmp
C:\Program Files (x86)\Hohi\is-1SPG9.tmp
C:\Program Files (x86)\Hohi\is-BJD6C.tmp
C:\Program Files (x86)\Hohi\is-O7AH1.tmp
C:\Program Files (x86)\Hohi\is-UTBJJ.tmp
C:\Program Files (x86)\Hohi\is-LT12K.tmp
C:\Program Files (x86)\Hohi\is-AT4P1.tmp
C:\Program Files (x86)\Hohi\is-LPP1D.tmp
C:\Program Files (x86)\Hohi\is-JLF4F.tmp
C:\Program Files (x86)\Hohi\is-BVPHV.tmp
C:\Program Files (x86)\Hohi\is-IP1CP.tmp
C:\Program Files (x86)\Hohi\is-LIJ75.tmp
C:\Program Files (x86)\Hohi\is-AN9G9.tmp
C:\Program Files (x86)\Hohi\is-EKIO3.tmp
C:\Program Files (x86)\Hohi\is-T6A2C.tmp
C:\Program Files (x86)\Hohi\is-D6K62.tmp
C:\Program Files (x86)\Hohi\is-B6Q9Q.tmp
C:\Program Files (x86)\Hohi\is-VQ2IN.tmp
C:\Program Files (x86)\Hohi\is-3K4EH.tmp
C:\Program Files (x86)\Hohi\is-2EG5S.tmp
C:\Program Files (x86)\Hohi\is-9UUNP.tmp

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

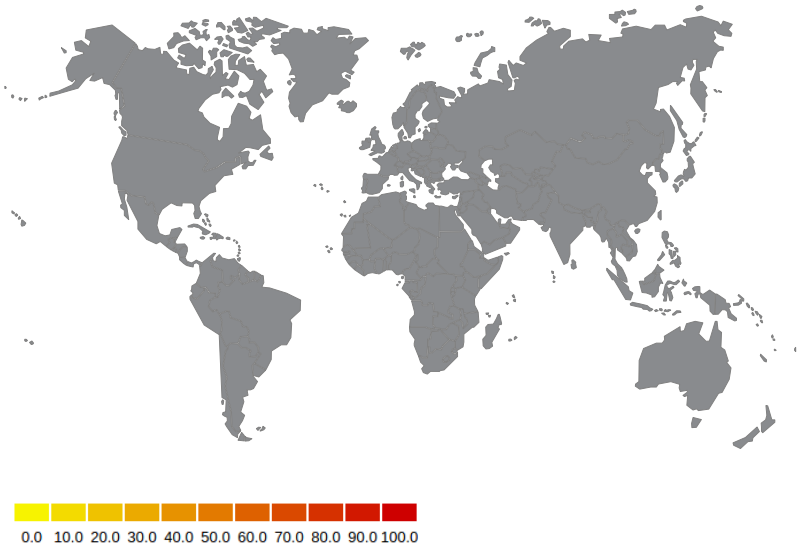
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
DefaultTabtip-MainUI

MODIFIED REGISTRY KEYS

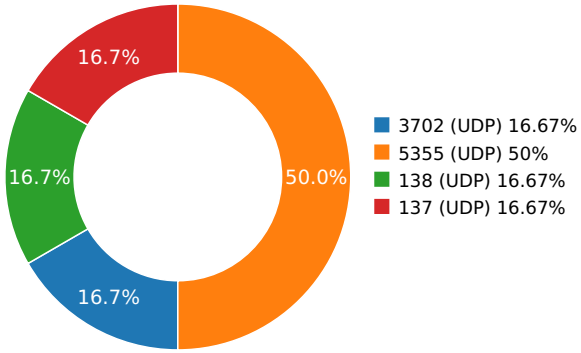
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\Inno Setup: Setup Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\Inno Setup: App Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\Inno Setup: Icon Group
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\Inno Setup: User
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\Inno Setup: Language
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\QuietUninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\NoModify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\NoRepair
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\MajorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\MinorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Hohi_is1\EstimatedSize

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.17228388786	Sandbox	224.0.0.252	5355
7.26638197899	Sandbox	192.168.56.255	137
7.30284285545	Sandbox	224.0.0.252	5355
7.31022596359	Sandbox	239.255.255.250	3702
9.86639785767	Sandbox	224.0.0.252	5355
13.3279128075	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Fanamek	**Type :** ASCII text, with no line terminators **MD5 :** af78f5ef886349df31ab12502f8d87d5 **SHA-1 :** fbb86d9262fbcdcae67ccd1871d7a73dc868adea **SHA-256 :** 8d33368c636c3927ef53b3f5eb6d5e0d1ff5c044d **SHA-512 :** c96f94e49aef88e704363199c0f99acec2e6168e4 **Size :** 0.126 Kilobytes.
C:\Program Files (X86)\Hohi\Kalolikade.Pps	**Type :** data **MD5 :** 839e119e71932a8abc3c3cc90309b4a2 **SHA-1 :** 04475c2a5c0fe54b4db6a1458af73de843e79c8e **SHA-256 :** ffe44eb5461d964d6e0549dad410ba5d6a30eb7c **SHA-512 :** eed4401d5e0b213db5ac8bdd9276c04c2847b70 **Size :** 0.745 Kilobytes.
C:\Program Files (X86)\Hohi\Fekas.Wpd	**Type :** data **MD5 :** 2adbc7ec4901fd1c995975f0498fe451 **SHA-1 :** 11145308d3d718b5dab7256a869379ece03a5c75 **SHA-256 :** d82be89e95a75b47e09ffd384fe4ec55b47305d8 **SHA-512 :** 691988ec5a45b8e605f531a8f320362d089847a4 **Size :** 0.198 Kilobytes.
C:\Program Files (X86)\Hohi\Pogalerehe.Bat	**Type :** data **MD5 :** 5f473afeafd2a4e61cd501394706ef8f **SHA-1 :** c8d4faafc5e1f7a66a789ac5d14ef2de667a1ee4 **SHA-256 :** 00d7b6664da5f66221b0ec6329546eb68e4fc174 **SHA-512 :** d7ec24f79e7004e46b1cd45f5483b473cba428ea **Size :** 1.025 Kilobytes.
C:\Program Files (X86)\Hohi\Petecaca.Mp3	**Type :** data **MD5 :** e108b658dc832f4e88db8eb482240a41 **SHA-1 :** a56db97f97f5f8d8630163446ee47eb351976e39 **SHA-256 :** f5ddcf7cd382a2ee729ac0fa93c79f4732002f2398 **SHA-512 :** 5e778c25c83ca806bb3fcdab2ccfd952c7eb8bfa3 **Size :** 0.245 Kilobytes.
C:\Program Files (X86)\Hohi\Rosakidek.M3u	**Type :** data **MD5 :** d92361f2ca7f43e34377a4a92279fc3a **SHA-1 :** e9e561a31a8fb32ae7dd48610de3232092f35393 **SHA-256 :** ce3f8fd9b7b404cc34f9d8328df5a1a58944f4c08c **SHA-512 :** c1a11065a77652616ddd6fa39dc5d11a5a0007a8 **Size :** 0.867 Kilobytes.
C:\Program Files (X86)\Hohi\Fofopagi.Hta	**Type :** data **MD5 :** b4a94a4d9ba4c18b45310f022618689b **SHA-1 :** 498f3e7431b3d70fd34f34f7c71c321db5a9756d **SHA-256 :** c10c332629f8e25d689e4c5935299724edd85d1e **SHA-512 :** 9140d13a942a8f61bcf34efbe67a8e415b5cb92bl **Size :** 0.163 Kilobytes.
C:\Program Files (X86)\Hohi\Fudepo.M3u	**Type :** data **MD5 :** 02a45437d4d1e886c487c22c6e587755 **SHA-1 :** 53e257676d552b8e0984576c2caebbd517175e92 **SHA-256 :** 518b52456ca8d921d3a9edc440fe9f3d069fcbda **SHA-512 :** 65d982fa35e00f56a59019fd14158d81fd63db74 **Size :** 0.249 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Fedocapo.Asf	**Type :** Dyalog APL version 11 .252 **MD5 :** b76b223053b84c229d36236307b508d3 **SHA-1 :** 96fff1d3c06e58b63953623034f9e203618e1907 **SHA-256 :** a12e902e7f3164b7c9ab8e3c9499ce6df6018d52 **SHA-512 :** a35c9d69a977b5ed7729b48b1a7bbc0304fa7e07 **Size :** 0.317 Kilobytes.
C:\Program Files (X86)\Hohi\Gopuses.Gep	**Type :** data **MD5 :** 927f4c3291714f8c060a46aacc4d30e6 **SHA-1 :** 7d80031acfbb21b1083a816e9fb7949d71b34a8a **SHA-256 :** cf3cbf4b60f721b471b7782bf3d47cfdb3be5f1bc8 **SHA-512 :** 3f453cb776cd8b3a231950b82e035311e5a14904 **Size :** 0.509 Kilobytes.
C:\Program Files (X86)\Hohi\Pamakomab.Cumi	**Type :** data **MD5 :** 4b3d60e349d413315a5f26976e3e0cf4 **SHA-1 :** 67dc2dba37a5414a535122983250ab58b5c910ec **SHA-256 :** 8a47e11e4e49e8c22c4794118e1a4ed2652c8094 **SHA-512 :** c994efa2db0252ba5c9c291825f0460c19776e252 **Size :** 0.327 Kilobytes.
C:\Program Files (X86)\Hohi\Dubepekadi.Jar	**Type :** data **MD5 :** 6c281aef04bc3c3d21ec3842a60169d4 **SHA-1 :** d0a5aa64dabec6a129fae6608b0db1ee7ece689b **SHA-256 :** 623d845f4b2ed330a9394d19567b3d226bf820f3 **SHA-512 :** e2d2f0862645420c19a4499ce23e6ef460be879ff **Size :** 0.993 Kilobytes.
C:\Program Files (X86)\Hohi\Hukakerol.Bat	**Type :** data **MD5 :** 5c5e254dc5353539654edd9cc1038bad **SHA-1 :** 65aec8889044503e81020fb53ca04cd6d48ed2ac **SHA-256 :** 165fd01e226de6bb6adfd5a17725e5c38bf13206 **SHA-512 :** 41b00b581dafaaa30208ec3a8282ca8ebc5daacc **Size :** 0.683 Kilobytes.
C:\Program Files (X86)\Hohi\Secafota.Sdf	**Type :** data **MD5 :** 80a3d3aa61210b1119b6d646974b0833 **SHA-1 :** 281cd232464ac501518be8ba45a86d1a7b0fe8a4 **SHA-256 :** 33c4dc2d008eefcea193003fdd610ed55e161cd6 **SHA-512 :** 416bfac61305f1a2f5fab8600d1dd18ad46eedd14 **Size :** 0.596 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-L8P07.Tmp\55bfa6aa04a16a892acdb2cc410192ab21e886a3.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 943dec64dd704964d5cda2029284d9c0 **SHA-1 :** 914ca8a04c07561ee6f77378d07999b31289529f **SHA-256 :** c7ef3efffb4d88c152fdb2a6a7102cd9e5867e35d **SHA-512 :** e2b8cb12375edef683dbdf4231b83b03f23787c4 **Size :** 711.168 Kilobytes.
C:\Program Files (X86)\Hohi\Ferebof.Html	**Type :** data **MD5 :** 28df351f0eae014a909613521a159c9b **SHA-1 :** 748dd9736da9da0084fc76af810ea8d4b64b21a5 **SHA-256 :** 65233450a7aae7dd8a83d9a7f7820b2a661cf5d8 **SHA-512 :** 662f293846aadab0b9bf908bec004f382b895be0 **Size :** 0.947 Kilobytes.
C:\Program Files (X86)\Hohi\Cemonokodeka.Kor	**Type :** data **MD5 :** 2c8a71a3111d728a478567f31bfdcfe2 **SHA-1 :** 390766c070874cdc36971d6a2496886b3ec4b8ec **SHA-256 :** ad31f73d6738fcb0daf8fef6dc8edfa45291e02dcc **SHA-512 :** 504dc0f4d398f1b2f675f353534b2530766056aeb **Size :** 0.104 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Fatulopapafa.Cpp	**Type :** Dyalog APL version 108 .226 **MD5 :** f6c639b9ec5c4c3a0e15b702f717bff7 **SHA-1 :** ad1e0127f808ff5c0706881b743c730bfeb59982 **SHA-256 :** 364b68ea46dd8e8739f5474b70bfc3fe3a3a7bcd **SHA-512 :** ba677818e141014789cbae4327ea58660804f39 **Size :** 1.096 Kilobytes.
C:\Program Files (X86)\Hohi\Tolub.Csv	**Type :** data **MD5 :** 4507c66dd65b8f6b07585e965c3c0815 **SHA-1 :** cb8226eac974af45ddc0b3888decb1f7b9f0418d **SHA-256 :** 7980b4e09b9fdc8d7857007b4f3094f8f210d719 **SHA-512 :** b772e21df2aef9efb5f9c007656fed80289a682c1 **Size :** 0.932 Kilobytes.
C:\Program Files (X86)\Hohi\Tusepof.Wpd	**Type :** data **MD5 :** 15f2750c9f531c431561c04a592e26ec **SHA-1 :** 1d55096251f60e6e904dfd0e5e30148a6bb59615 **SHA-256 :** 09f26dcfd379ca79f848187ef0cd2e01ac7043327 **SHA-512 :** 892901d7035796860e659870874555df1d020ec **Size :** 0.505 Kilobytes.
C:\Program Files (X86)\Hohi\Tecedus.Com	**Type :** data **MD5 :** eecb76e83d2b920c15058f6c468121cc **SHA-1 :** 03fe2c7ed710c89613cdf7f8f2255b0560f562b5 **SHA-256 :** 105a4dc882de33a82c7ceb358362d4d045be4fc0 **SHA-512 :** 928ad7fb9e8f793c5b749c122a0f704b4fe3ae8b1 **Size :** 1.115 Kilobytes.
C:\Program Files (X86)\Hohi\Unins000.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** d30bac5269d2b7fb33a041721a4dc353 **SHA-1 :** 12bfc67e9525d0d7842c8f0fc7bbb72ed0c7ed18 **SHA-256 :** 5a5596a2ae2859ca9e6751659e3b3e129148307 **SHA-512 :** 38b99851c7aef54a471a5d2fcb6251aa86f7e324 **Size :** 722.597 Kilobytes.
C:\Program Files (X86)\Hohi\Lofolado.Pages	**Type :** data **MD5 :** f5243fb061bb2910c5789731ecfae9cf **SHA-1 :** cc9c9f9e91702932e5bc551d8d637f36b12d6818 **SHA-256 :** 318a394a19420744f18225ccbfb7981b0df143e1 **SHA-512 :** 4e021915f967a7a91c1304c61417150ca0a4e527 **Size :** 0.923 Kilobytes.
C:\Program Files (X86)\Hohi\Moruf.Ke	**Type :** data **MD5 :** 51fbbafce5b1f1d7a9bf0f9c497bb91c **SHA-1 :** 62cafde48d3e19ba2eb44e3e5d8e59dff8aecd11 **SHA-256 :** 9de0ac8f080610595421c46d0ea6e5130f04afea **SHA-512 :** ab342d79879268e5b6d8ef10c159b4758c43428 **Size :** 0.507 Kilobytes.
C:\Program Files (X86)\Hohi\Gohukanasosu.Hta	**Type :** data **MD5 :** 1253f4cadd3e6cfa5ff6eecc080fa8d3 **SHA-1 :** 7f72d21dbfd41c69b3168357f39dd6c2c2075a60 **SHA-256 :** 8bdbbf213000ac462dc4643f34694344bd032ea5 **SHA-512 :** c99da9535d6cfd8cfb29110442f9ba144c42f0a68 **Size :** 0.153 Kilobytes.
C:\Program Files (X86)\Hohi\Cekocamod.M3u	**Type :** data **MD5 :** 9c92536e6e97fda5e106cd6a1fd3ab95 **SHA-1 :** 4649c921b36f19cbb17ef3c1b1d80ce88c89d6ea **SHA-256 :** 43082196f5c5335ea2094ed2b3353da0a98be14 **SHA-512 :** f8a734e5db8da12ea4ef2a481163a7b37f24f9c21 **Size :** 0.516 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Puritocon.Ppt	**Type :** data **MD5 :** f73395ddcf158d22e26360eb9094b6e6 **SHA-1 :** 74362f2ab0c6a4eafcf049717a23d33d9914fc82 **SHA-256 :** 111a002cbf290c156d131ecf08b339e374234712 **SHA-512 :** 7fb489cb31650fe30e986c2edf28902bb753d3eb **Size :** 0.466 Kilobytes.
C:\Program Files (X86)\Hohi\Bepagucib.Com	**Type :** data **MD5 :** 0f5a3e1bc02e80f553e7a7d44b209146 **SHA-1 :** 55165094f672415942b4889917bc920464a7e691 **SHA-256 :** b8b534f7b0f84f1a39b96456c90ef7ad1a814224c **SHA-512 :** e51c27c16619d649898274f18a2ef18c848754075 **Size :** 0.641 Kilobytes.
C:\Program Files (X86)\Hohi\Nomof.C	**Type :** data **MD5 :** 4e0e34616945c8147a19ad33cd8d8a38 **SHA-1 :** 1566f34e75856809e784a7ac67e5d01fbc4489ec **SHA-256 :** 07c1574e5f2b1bf72afc41df7b29029f9f1eb0e413 **SHA-512 :** 929646232e23bf70cf64abc1695e44369ed5fba57 **Size :** 0.351 Kilobytes.
C:\Program Files (X86)\Hohi\Nifob.Rtf	**Type :** data **MD5 :** 9b5ed3e46d998e9ab220f66cb8b78f05 **SHA-1 :** 6f282635bd4ec03f8cea267ef455f04f28eb0a51 **SHA-256 :** 7dc1ba539b91d81f41da496158c9b08404da2e6c **SHA-512 :** 4e5b2a9c52569acbf1c72fd20a940b6ba84682a7 **Size :** 0.288 Kilobytes.
C:\Program Files (X86)\Hohi\Funagub.Exe	**Type :** data **MD5 :** 6c478fcf0318dc46e41e0a6f906ecf3a **SHA-1 :** 5876e1a33953a0aaf8f29d6554e03be13985df79 **SHA-256 :** e0bc02c06680d1e6f68cfe5ca0a4040c9d840b9c9 **SHA-512 :** a15a99f35afb0b1791864ae99cdf4bb5408f5a7d4 **Size :** 0.426 Kilobytes.
C:\Program Files (X86)\Hohi\Sasetef.Vob	**Type :** data **MD5 :** 2f155bd5e02898f42a606e058b2fb14d **SHA-1 :** b1a30bf37fcf5fa4fcc9bf0068b00a2184d96174 **SHA-256 :** 0746c519ea57257698b349d8aee53aa67505a993 **SHA-512 :** 83a3341070c6173ac0c50561d7f033012120e275 **Size :** 0.335 Kilobytes.
C:\Program Files (X86)\Hohi\Hoguhehefu.M3u	**Type :** data **MD5 :** 70dadd5f9364f198c9013f27ec828d08 **SHA-1 :** 2c86d197dcd3d821ca2d0718ad29650857e81f9e **SHA-256 :** 3b05dba1d7b32c16bd319f3b543a1bc43726f1b1 **SHA-512 :** 5ae638b84aa60d26c89163c4bcf28748062088f7 **Size :** 0.75 Kilobytes.
C:\Program Files (X86)\Hohi\Dusotedam.Html	**Type :** data **MD5 :** 0c11294958842aff0ff4f811052594c1 **SHA-1 :** 99467eca1344d703459879ce5c617f07c58cae2c **SHA-256 :** 78a7d8118f28a0892482a47f2c7f7382fd70fef021 **SHA-512 :** 58a01e257f2854929c3ac6c115f865d1c406233e3 **Size :** 0.693 Kilobytes.
C:\Program Files (X86)\Hohi\Fusab.Rtf	**Type :** data **MD5 :** f890c026eab60d456d740dba641342fc **SHA-1 :** 85ffc42feefcca3e147bc23ddf2c8cd6e8b3e6c8 **SHA-256 :** 070abad49fbba24325cbb94c138766b35e36ebd **SHA-512 :** aa591dd25439e22e5290f46c5447220473efe801 **Size :** 0.523 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Gupaf.Hta	**Type :** data **MD5 :** 7c073157f6456991ef8617936a146b6a **SHA-1 :** adc5bece0a6c89c4e7acc330cec806c58c46cac5 **SHA-256 :** 56037aa7ebabdd11e5032ffe3c6777df795abd67 **SHA-512 :** d5e4eb00f947275b20ef061aee42da1b1226a1d2 **Size :** 0.424 Kilobytes.
C:\Program Files (X86)\Hohi\Cufepubo.Com	**Type :** data **MD5 :** 7820baaed80bee68e17ec5a05e78911c **SHA-1 :** 0aff6e13d86b4bbf895a06a2214da645eaf239e1 **SHA-256 :** 4f51071468d6327907c2d347a854be382ac872b6 **SHA-512 :** 52377de1266fedef3b9b9dba46c51c7a8ec740ea **Size :** 0.264 Kilobytes.
C:\Program Files (X86)\Hohi\Pahebohabos.Ppt	**Type :** data **MD5 :** c128a89dda8510e3e6407af95fc15e75 **SHA-1 :** 84d0983a433984776c2fc587f673db5bf6326046 **SHA-256 :** b419da0751dbe737b9dd52fe09a0e5ebc842215 **SHA-512 :** 1bfbcf214cbb053d28fa8629bc69e70f771f5bc6b **Size :** 0.323 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-53TKA.Tmp_isetup_shfoldr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 92dc6ef532fbb4a5c3201469a5b5eb63 **SHA-1 :** 3e89ff837147c16b4e41c30d6c796374e0b8e62c **SHA-256 :** 9884e9d1b4f8a873ccbd81f8ad0ae257776d2348 **SHA-512 :** 9908e573921d5dbc3454a1c0a6c969ab8a81cc2e **Size :** 23.312 Kilobytes.
C:\Program Files (X86)\Hohi\Foboce.Txt	**Type :** data **MD5 :** 9927376da2c5b0c435a8d879166ef572 **SHA-1 :** 2ed8a5b125b85a2fee7d5357df66ec51fc1d833f **SHA-256 :** af7767b514c5308f6ac752295d0e50628e1b36a9 **SHA-512 :** ca188e0bbf72132399f5a2d92a419691738d72d9 **Size :** 0.995 Kilobytes.
C:\Program Files (X86)\Hohi\Keber.Mp3	**Type :** data **MD5 :** 9ddf62f3727cbc81e03c82225ce7a11f **SHA-1 :** eb7145cf3ff392a6de81d1bcfd81711ae7c1417a **SHA-256 :** b54ba520d63067ab643d282583016aab994288(**SHA-512 :** ae5cd731be13afb386c5d3dc7f70e5e1f73dd942 **Size :** 0.701 Kilobytes.
C:\Program Files (X86)\Hohi\Decodusehupi.Log	**Type :** data **MD5 :** a3224c53495cb9f3b4f043562ff43951 **SHA-1 :** ab8ec8078627c48695026cafae5be3ad08d39280 **SHA-256 :** e03e1ec9f3ea30e0b3acbce5266aa194b1008359 **SHA-512 :** a8c8200308bb5afc2c18566b3fb13bcf1c7124cc0 **Size :** 0.674 Kilobytes.
C:\Program Files (X86)\Hohi\Micer.Hta	**Type :** data **MD5 :** 30fd29c637a3c3d87c6ca0e1e1bf11cb **SHA-1 :** c03154a98b35c3549b313c6c003aaa59477c066d **SHA-256 :** dd4d796b625697ed1102a9a03a9d3462647112 **SHA-512 :** c1f745d7d3274fea98234a6c17d50c0c3510ee50 **Size :** 0.471 Kilobytes.
C:\Program Files (X86)\Hohi\Dacafola.Pptx	**Type :** data **MD5 :** ca5c968521cfca1429c4e58217384430 **SHA-1 :** 7f5be5d5a37031c61c6210e4f4f0778caf015003 **SHA-256 :** ca184695ec4a97b05788dd9d6c0776710579c9ef **SHA-512 :** acdaf1d88aa7d681f6487af39d2dfc412d2e1e81f **Size :** 0.436 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Narip.Msg	**Type :** data **MD5 :** b274ecb22f8da494d3efd6f980e8b959 **SHA-1 :** ea6669358161598115406 92ef15c3aaedb9518a6 **SHA-256 :** 7c2184f06ed039633daeabc2002c2cec5cab6108l **SHA-512 :** 222413ed74275364cc299173079b6b2508ffd552 **Size :** 0.557 Kilobytes.
C:\Program Files (X86)\Hohi\Tutopidom	**Type :** ASCII text, with no line terminators **MD5 :** 6141d12290fd74c1e92c4102b2077871 **SHA-1 :** f2284783321cdf01ad171f35189ef6291b95fb44 **SHA-256 :** d3cbf34c61a2f5409de04f4eef4ecd9a41ede504f **SHA-512 :** 7fa3b6781eaa0fb0f626b844202a4d02b5eae27f4 **Size :** 0.133 Kilobytes.
C:\Program Files (X86)\Hohi\Caluselah.Mpg	**Type :** data **MD5 :** db4dddcb836ab8230c2eda3b975be131 **SHA-1 :** 13327c2e5d37bdb7306f0d9dfeea869e744c425e **SHA-256 :** 74ac0e63a04d7f5726f9e2d203a009314a224a7c **SHA-512 :** c1b10fc571146913c89eeb7c72715b156397641d **Size :** 0.956 Kilobytes.
C:\Program Files (X86)\Hohi\Curul.Tex	**Type :** data **MD5 :** eb1c8ad932da9c3ee44b3c49fe3ec721 **SHA-1 :** 58ec05485cc72723bbeaa64d4955f4ea3ba307e1 **SHA-256 :** 8f46f4f7995892cb7af0fd83ca51ed184e0ad1450 **SHA-512 :** 828aac8db6619d4f85d90ea4dea75e872b3ff083 **Size :** 0.275 Kilobytes.
C:\Program Files (X86)\Hohi\Noheninened.Bega	**Type :** data **MD5 :** df93f5228a9c07a700e96fdd95b47e27 **SHA-1 :** 05f2d974d2a7c051ff52f68f931d7a5957650d5a **SHA-256 :** f99e2ecce62269b385a929356358bac2ff05b710 **SHA-512 :** 36dd947151d991696e1a6a04f37f26bfc26c7fc60 **Size :** 0.154 Kilobytes.
C:\Program Files (X86)\Hohi\Kasohu.Wpd	**Type :** data **MD5 :** b12a1afb0a6ae70d71370efab5d55b9c **SHA-1 :** f1c99393493849c7361cf2d9bf690e4ec3c53a92 **SHA-256 :** dc45f64e85d89459f31af801671cca25675aba53a **SHA-512 :** b75451392ccbe55629287ba055fb28a962cfb35d **Size :** 0.418 Kilobytes.
C:\Program Files (X86)\Hohi\Latupubap.Cpp	**Type :** data **MD5 :** 3161ec06cfa8ac81de731e7edcc747da **SHA-1 :** 9a8769009d2496dffadde09fa7d9a3ab56b7a64e **SHA-256 :** 3b85dc03da9848ab9f6481bce56ee77b882303e **SHA-512 :** 599470438035598bb356b266b14d9768f3f2a24(**Size :** 1.036 Kilobytes.
C:\Program Files (X86)\Hohi\Podegogetog.Vob	**Type :** data **MD5 :** e08a52475487719dc188e40f9fe16389 **SHA-1 :** 1aba580c0c6bee47005399613523a196f162eabb **SHA-256 :** 96bc39c33f0522b60bf831c7894aea92f28bd9b7 **SHA-512 :** d3e81b23e7ad18d0c89809b2e2785898d931863 **Size :** 0.231 Kilobytes.
C:\Program Files (X86)\Hohi\Siracatusem.Nesi	**Type :** data **MD5 :** ccab24e660151d839cbd1b77b1bb9b03 **SHA-1 :** 50e5e0aa4c592c2654e8770bdb54d5a5928fd55e **SHA-256 :** d4ebb318fe94a3ee045a0244baee2403b159e59 **SHA-512 :** 622d22de4f5e67071a4104c83b3e8346ea9dc5d7 **Size :** 0.542 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Lefag.Exe	**Type :** data **MD5 :** 23d29f59d5c9024482804a2b5e23aabd **SHA-1 :** 0c1d320c2bb6dac322c09d20915814e91ed0b80c **SHA-256 :** 383609652b28ca077083ab8cf3f3238445eca5db **SHA-512 :** 9597120f90220245c9f000f66dd8ca737a661854 **Size :** 0.708 Kilobytes.
C:\Program Files (X86)\Hohi\Cikasipo.Vob	**Type :** data **MD5 :** 0cfd7d493c1665aa6d3a6a4269920017 **SHA-1 :** 0f447475ee1b88218c76c6aea9f9da915a036aed **SHA-256 :** 3689b570204769ad6dfb06363d08580085c2173 **SHA-512 :** 212aace3c1d8ea0c4fa16118b44c784f635971b3f **Size :** 0.951 Kilobytes.
C:\Program Files (X86)\Hohi\Unins000.Dat	**Type :** data **MD5 :** 83f63da3b567b72361a07ac16a2eb75c **SHA-1 :** 53979b8657ff51051962e44672accdde170695c1 **SHA-256 :** 2b8d056eb368308d341871f37c44c74eb9e436f4 **SHA-512 :** bc5b7347fad37bffe98222d253c4ffa7998008017 **Size :** 6.638 Kilobytes.
C:\Program Files (X86)\Hohi\Mecekolid	**Type :** ASCII text, with no line terminators **MD5 :** 3937bbb613eab4027be5b806d0606381 **SHA-1 :** e4b8fd5538ccc5b93068bd5dbd6a7488a77f80da **SHA-256 :** 4ffc3b7d54dd789ca3444e332ddd22e6fcfbb3b5c **SHA-512 :** c44fa58f2ef26bd56161ee59449a05396b42e376 **Size :** 0.132 Kilobytes.
C:\Program Files (X86)\Hohi\Supulerof.Csv	**Type :** data **MD5 :** 71d6f122622a49e9076718333d57f358 **SHA-1 :** 75455eee15d8cb9b87a0205f26edfe0d1b18310f **SHA-256 :** 4855877b7b316b90cfffb06d5098ae82e91b4fe9 **SHA-512 :** ff7d016c666a057b4bf20b61c90f8d681f03666b3 **Size :** 0.589 Kilobytes.
C:\Program Files (X86)\Hohi\Rokicaha.Exe	**Type :** data **MD5 :** 64a68ec6303813bb8bea3c002d7b6b26 **SHA-1 :** fb0765cc219e49500f5bca084c1df9403b752606 **SHA-256 :** 2b090062cd5de1d0ef5ff7be19c61b3b0cb2189e **SHA-512 :** 37f0fa85e7669759ae8f44a1678d89b561b183f4 **Size :** 0.352 Kilobytes.
C:\Program Files (X86)\Hohi\Rukunododor.Odt	**Type :** data **MD5 :** c7acf96700c188d05f8ba00f166d2950 **SHA-1 :** 5fd6961e18c7bf69ca6833573bc60c0b8452eb98 **SHA-256 :** 6deb0a7d5aba8a72f28403391a1fe755e33bef59 **SHA-512 :** 2d0d7b6c478c4ea9751e6fe43ea1671d113280ae **Size :** 0.819 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-53TKA.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba **SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc **Size :** 6.144 Kilobytes.
C:\Program Files (X86)\Hohi\Tehitogan.Wav	**Type :** data **MD5 :** 6bbb851f78d24c2ecb1a6f71f4d8946d **SHA-1 :** c90afc3471948cf38cc23ac4619a05b31d888bb9 **SHA-256 :** eb6e7e5f8ea6e2a2044698bf1e1f7dc5c6c040501 **SHA-512 :** 24908206926904e9a56e7a43b8788fcab63447ee **Size :** 0.313 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Rolamuga.Fat	**Type :** data **MD5 :** c6b8f74a64f48dd47eba41b2a020fb04 **SHA-1 :** 113881bca1e0efbf9081174fa08cd3ecde60ae0d **SHA-256 :** 220429d692fa2c972c8b9f7b066e540ab3d0929e **SHA-512 :** d7c33d3f81309499004a552d220b2ed3fd90a117 **Size :** 1.114 Kilobytes.
C:\Program Files (X86)\Hohi\Fegebag.Wav	**Type :** data **MD5 :** f6d86e0f6322224d3a9c9ff2d7965575 **SHA-1 :** 8d3dab08e75411154a19cf232f0694dac64cb0cd **SHA-256 :** 8772a6765e2ee20869fe01b2fb8be795c9c0c99a **SHA-512 :** 6661f8b77b5b61fe457440373f177dd297a0e419 **Size :** 0.1 Kilobytes.
C:\Program Files (X86)\Hohi\Saserel.Xml	**Type :** data **MD5 :** 9093f29a120b17b8e8bfbe298f1b9b3f **SHA-1 :** 32fb0b58f659a6eab75a534ddb95362bc9718680 **SHA-256 :** bfe29488d4795bbdb1a9bcf7fe19aaeee67d73fd **SHA-512 :** 2f121e5e810a58e767c9f24e503a0ae98eb9245b **Size :** 0.291 Kilobytes.
C:\Program Files (X86)\Hohi\Halikog.Ppt	**Type :** data **MD5 :** 15bb623aca5573030c01b037080ec59b **SHA-1 :** a030307b6f0ddf22f54bcb4b3671f1f91bed6542 **SHA-256 :** c3ab9b14bd783e78b6d17ef6b12f760901deba7 **SHA-512 :** de068052a3b1d8b0fe5540a045b2ae190fd931b5 **Size :** 0.984 Kilobytes.
C:\Program Files (X86)\Hohi\Kelanu.Pptx	**Type :** data **MD5 :** 0b38ca8f70afb6b3b70d77cf9ac28369 **SHA-1 :** a5784a510b8079fe00592153918eb8b1f911792c **SHA-256 :** 5824f563870b4036ed6cde1e5e873e90ec38d807 **SHA-512 :** 250f5f72fa661582ea1ea559dc917ac8ee43d4fa2 **Size :** 0.194 Kilobytes.
C:\Program Files (X86)\Hohi\Nepekinulud.Mp3	**Type :** data **MD5 :** 7b51bada117f273868418fef5745b0eb **SHA-1 :** b74c5380d5c482a541f29832784eac802868c155 **SHA-256 :** a576ba7d55d6baa6b963dbd32345a1e7d042cce **SHA-512 :** 50d36326561c538b3802ca717c00510bcd3e6c45 **Size :** 1.095 Kilobytes.
C:\Program Files (X86)\Hohi\Cofago.Car	**Type :** data **MD5 :** 6ce0779bd5e130133f147ea59d3ce0c9 **SHA-1 :** 371ba0745741d7ef30636058eec4ee2471e2c97a **SHA-256 :** 13395a1f2d725b6ea2693f985630d4856a1e2b5c **SHA-512 :** 68244bd339ae4aed87d3e4fb2779cd0975e9cce5 **Size :** 0.679 Kilobytes.
C:\Program Files (X86)\Hohi\Hupanane.Odt	**Type :** data **MD5 :** 7763de5d3b4b85b23d217c102df2deba **SHA-1 :** 5349929cc461f8bdc4e2ad597077fa4803186ac1 **SHA-256 :** aa1d2f3a2d48ccb97eb963cff6162003d4802fe2b **SHA-512 :** 3704069574ad743d54ea29bee1dab85f5b8a905 **Size :** 0.703 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Rabarop.Html	**Type :** data **MD5 :** 54927723d947ca0fcba6b941e413159e **SHA-1 :** a68a864df28b4cebf7aa86a16a1c644d6867bc06 **SHA-256 :** a9ddbf4239d32c818e647984dce32b4bc6dea14 **SHA-512 :** 3cb60b78ed33841ddc186e41be000de8d8180e6 **Size :** 1.115 Kilobytes.
C:\Program Files (X86)\Hohi\Lireta.Csv	**Type :** data **MD5 :** 8ca002f6054c397b59d025805a18489f **SHA-1 :** 1b45f4ae642e059c052301f95ad3bffb60f23e49 **SHA-256 :** fcbc78ead087de825d15080699fae366a3f02d56 **SHA-512 :** 01928bdf2edf7cee9557415b92fb50f0a5906596c **Size :** 0.869 Kilobytes.
C:\Program Files (X86)\Hohi\Mikefudeha.Doc	**Type :** data **MD5 :** cdf686ce52da7e1fa03bbcab881dfddf **SHA-1 :** 7e257c42761dc8c9098d0dc4fba0d9f09d67f2f9 **SHA-256 :** 5cf2d6e11d166baa125dfeee39fa7b788526381e **SHA-512 :** 833e98ff1782cf2ca0c91afc9f496794508ceee2dc **Size :** 0.96 Kilobytes.
C:\Program Files (X86)\Hohi\Tucob.Xml	**Type :** data **MD5 :** 5c0c9b0cd8b8d95d5d1e3b882f245798 **SHA-1 :** cbd736ffd7e08c6f48c8232f2de1bfca0bf1ac4f **SHA-256 :** e1fca88bde3bbb7481775d81f7da4182c6e44419 **SHA-512 :** 94b5f7eae8963055c8968ebbc9b651d7975dc557 **Size :** 0.872 Kilobytes.
C:\Program Files (X86)\Hohi\Dulosilaru.Wps	**Type :** data **MD5 :** 144b844493fdcb91a19c29652109ab26 **SHA-1 :** 2fe0fb6f76b6a2882595cea6fbfe6fc34e57d4ef **SHA-256 :** 659d6e8ae219ba7dd52e2b2e826e2de8815c461 **SHA-512 :** 214594fc0597e4e79456b05a1b00607070a6f8fb5 **Size :** 0.759 Kilobytes.
C:\Program Files (X86)\Hohi\Hameguludo	**Type :** ASCII text, with no line terminators **MD5 :** 48ad2d8e0f0c1674f35f976e0d122563 **SHA-1 :** 8699a83032e063ab92e62bce6587810103610bda **SHA-256 :** 82152d8040e0649db1eb66653c2710841167122 **SHA-512 :** 0f0bc993ac4ee168cdf80009521ef58254f67d307 **Size :** 0.135 Kilobytes.
C:\Program Files (X86)\Hohi\Ciberalina.Html	**Type :** data **MD5 :** d858f12c2287449b4fa76bc892d62bb6 **SHA-1 :** b93d89a5478fd2bf6c1705decf5c868673073acb **SHA-256 :** 1ccaa429db778f47ad1be11640a4048564010d27 **SHA-512 :** 5987e56328e738d3b930fd3a388fe2d1fea22229 **Size :** 0.594 Kilobytes.
C:\Program Files (X86)\Hohi\Ginokohates.Ppt	**Type :** data **MD5 :** e077f8c2edce9c7dc0bcfeef55392cf7 **SHA-1 :** aff9c3211ae46a585279ec08560f5c109ed8d20d **SHA-256 :** e7706a790288f6049900dcde3432938380419e01 **SHA-512 :** f318170dbf684925d8fe792a03563fae90af01eb8 **Size :** 0.317 Kilobytes.
C:\Program Files (X86)\Hohi\Gulag.Wpd	**Type :** data **MD5 :** b515f35298d03f2705be28101bfa6ece **SHA-1 :** ac0cee7d9ee407e2421db18886300d9130949b61 **SHA-256 :** 3be5da0be68fad8969d361f4c0c93f2cc657e375c **SHA-512 :** 52aec6e312feeb174a141336d3b8e2ce13f439f8b **Size :** 0.91 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Guhiko.Srt	**Type :** data **MD5 :** 3666e43e4d5951b4221522aa8cc553f7 **SHA-1 :** 76ca62bf15abf15515386597538d03c4cdd808b0 **SHA-256 :** c917867316069555068e3b2403aedbca2206a2c **SHA-512 :** 21738f47c57e25c9a5561d954220d4f9a252318c **Size :** 0.137 Kilobytes.
C:\Program Files (X86)\Hohi\Keganocasi	**Type :** ASCII text, with no line terminators **MD5 :** df89fa61a1a5ea3fa7c9a550045e3a00 **SHA-1 :** 99e3885ebdc6c4e85d66b92e0dd8ec8a5d42d706 **SHA-256 :** df4447ea1246e8ab4b4392a5cdc7c6f8fca0f1174 **SHA-512 :** 45e7be38afde1d5bc1ff28cd2715b9bdbb1b82bf **Size :** 0.126 Kilobytes.
C:\Program Files (X86)\Hohi\Kedonukepini.Jar	**Type :** data **MD5 :** bece855db5c088d7129db29cb360b6ce **SHA-1 :** de69daea364d887b6578d0d2bd7d84c7155204a8 **SHA-256 :** 880133d4596cae281e1aebec1999e6820a5d408 **SHA-512 :** 2aa8e25d786aef3595c970e49e391138bf885287 **Size :** 0.452 Kilobytes.
C:\Program Files (X86)\Hohi\Logacodol.Com	**Type :** data **MD5 :** b7fc62cbe3879756cb27e5d6e749e5f2 **SHA-1 :** 88f9cbc218a74df530cc1e9fc42f1ae2c45a36d6 **SHA-256 :** 312a40b2d465b62f7c06c5eafbd9c51de313d8c0 **SHA-512 :** 31bfa7b401fa4911935af836df42560e1c1f62539 **Size :** 0.648 Kilobytes.
C:\Program Files (X86)\Hohi\Nepodec.Dat	**Type :** data **MD5 :** 2bbbc8a5621eee08cc30aa8859743397 **SHA-1 :** ad5ce4ae938e06356f37af12480dd02b0028dbe0 **SHA-256 :** 3af344efc1478659ad8a011e204094c510e25234 **SHA-512 :** 2c6c03e7d1faeb9fdf74976ad41502669ec25b0df **Size :** 0.728 Kilobytes.
C:\Program Files (X86)\Hohi\Dilebenet.H	**Type :** data **MD5 :** 8daa131d451af5181cac9b02c30bfc75 **SHA-1 :** 5126f7cf0dc0982120a28937570977cf4d85e24e **SHA-256 :** dfbaa2d2abcc1087463a37e36c3cdab44c51f587 **SHA-512 :** b093f196a6844bb74b829b888b9cf965e9ef67c3 **Size :** 0.359 Kilobytes.
C:\Program Files (X86)\Hohi\Parep.Pptx	**Type :** data **MD5 :** 9a101a2d264d78fd4e40d1d698cf6143 **SHA-1 :** 4e95adcf0dec8851e7523c3c6caf1ccffd700b89 **SHA-256 :** 21345320a2fdf1e1045d5a6de88e3386a41be15f **SHA-512 :** 8191c81218354bd936e37dd4b31afea41f2b7821 **Size :** 0.871 Kilobytes.
C:\Program Files (X86)\Hohi\Cedade.Jar	**Type :** data **MD5 :** 7743dc862062508666a7b7a6578394eb **SHA-1 :** 62c6f1724131479ae9adb7683b9cb4e9d6f72b76 **SHA-256 :** b9e49d5905533bf65a47b92c853c6e215d3a3fb0 **SHA-512 :** f72e2af58e7b2c4f8412ed5da494bd4c89d2f74a5 **Size :** 0.535 Kilobytes.
C:\Program Files (X86)\Hohi\Linegori.Sdf	**Type :** Dyalog APL version 44 .156 **MD5 :** 6a03f7bb940d847d20e0778de16148c2 **SHA-1 :** 5b13d53ff77fb33771998afc43cddb0ba9c9619c **SHA-256 :** 1005fad99c24f70f5e4cb2956960e51460d3a4b6f **SHA-512 :** 0b12ac6faa67e27111375b5e8679f3898967ff2b6 **Size :** 0.939 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Molenep.Html	**Type :** data **MD5 :** af8afa5904bd7412c7879936da9f8767 **SHA-1 :** 3c9a01aa5fee485a5468cd73d644d8943ac9b015 **SHA-256 :** 9e25cbd25aeab1959d1fc1b06de9c706ab3729b5 **SHA-512 :** 9a11c86451da15cfa6f5ab894064c942e248bb28 **Size :** 0.261 Kilobytes.
C:\Program Files (X86)\Hohi\Godudogibodo.Txt	**Type :** data **MD5 :** dbc7da296c09308dbab526913cea682b **SHA-1 :** d668d0b050c659ced5d6f9b7fe52355cf3725893 **SHA-256 :** 4c6c6f2ef059fdf86578e9f98fb9a734d9dd1268ee **SHA-512 :** 024c91a6d400356702f162b77960c358c13df2bb **Size :** 0.158 Kilobytes.
C:\Program Files (X86)\Hohi\Gikocub.M3u	**Type :** data **MD5 :** 947a7677b48c0b808846b4281a0af7b2 **SHA-1 :** 6912b7f888f247b768169fe629f27f31c5a9460f **SHA-256 :** 35b9c7aca3eae03d80678417dc98b5363875c77c **SHA-512 :** cf3c703eba5192aa59136877642ffcdad9b0ef07f7 **Size :** 0.237 Kilobytes.
C:\Program Files (X86)\Hohi\Rebasomahu.Doc	**Type :** data **MD5 :** 008db2b5a88ee6a3e788aed8da9ba2d8 **SHA-1 :** 9a982066a44fe42407247797de283b8d49c0662f **SHA-256 :** 714651ebeffa6af53799a244497270ea6902d140 **SHA-512 :** d4416f8aece3168e9b8c6934e355e34b6a52b777 **Size :** 1.117 Kilobytes.
C:\Program Files (X86)\Hohi\Nomagitop.Cpp	**Type :** data **MD5 :** 0dc3320c0f268c3514ad1abe75b2e46c **SHA-1 :** 78f2eac85794be1b52693194c53e49d81f4bea10 **SHA-256 :** dc3a6841ad78c8087a439c7f73123d44592fffc63 **SHA-512 :** 833b45eab9459c3455e050745a3be09e0f71ef57 **Size :** 0.318 Kilobytes.
C:\Program Files (X86)\Hohi\Cecudagede.Log	**Type :** data **MD5 :** 06d0b05f4f319583f01bec931fc584cc **SHA-1 :** 75fdc01fca4307996c0e9fc4c1667d8300477b08 **SHA-256 :** 40a9d0f8f8e61dbdd916338c84859e88ff4a3cbb9 **SHA-512 :** 4a0b5c6f98396792ff4c70e118c552449d4625817 **Size :** 1.096 Kilobytes.
C:\Program Files (X86)\Hohi\Kibibemonuru.Mpg	**Type :** data **MD5 :** 4ed77a084847bb3971e8209680ab167b **SHA-1 :** cf8c60d4a094664be519cc41cc6e606c18da33a5 **SHA-256 :** 8c695372f3e7b1674446a08869bfcb1f08abf16b9 **SHA-512 :** 9e9c3a9bcada0a4784dd2885a16913207276b5f8 **Size :** 0.267 Kilobytes.
C:\Program Files (X86)\Hohi\Delihog	**Type :** ASCII text, with no line terminators **MD5 :** 83a4bac7f3e10a11842c8d8349d63f0a **SHA-1 :** ca9256d83d02a29bafac65b86b88e1e0af365fd9 **SHA-256 :** 657992c7ed82b8c3a8ff3583e40533d3ba4f2aee7 **SHA-512 :** 0e1639e4e8aeaa5c157d4e5a663ff9ac143ffd7e0 **Size :** 0.186 Kilobytes.
C:\Program Files (X86)\Hohi\Lepim.Ke	**Type :** data **MD5 :** 190c043e5aa095d6f32299eafb0d23af **SHA-1 :** b3ad219fbda0f6aa4bfc40c790ad63362484d4e1 **SHA-256 :** 7b4db78306df5571bd0134e959ad315959c5e41 **SHA-512 :** 0babcd62d604d04cc4aeed486fabcff5142616e3c **Size :** 0.719 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Kenigasakepo.Vob	**Type :** data **MD5 :** ea71b7b8088f7702ed25b6f92f74472f **SHA-1 :** bf72e63d3471ddaa2494a95d3dc8e5fa5801704d **SHA-256 :** 33d072a80a1a3a895bc7782c0a95b60ef9701f7d **SHA-512 :** fd386a8b2d63b60c853ed4d131648d900c56af79 **Size :** 0.418 Kilobytes.
C:\Program Files (X86)\Hohi\Kafac.Hta	**Type :** data **MD5 :** de0928d272200ab4dd64794baf46e7cb **SHA-1 :** f358f01dcb44dbffe94c54a01000c331c17498ba **SHA-256 :** 21aa5982dac509213839769ea87ebbff244834cd **SHA-512 :** b46bc7b20f038fec8b1176c1c77d9fdea002fdb31 **Size :** 0.341 Kilobytes.
C:\Program Files (X86)\Hohi\Dalasekibupo.Bin	**Type :** data **MD5 :** c632c83f476f5dba8a314fada4ae2129 **SHA-1 :** 192c9fc821ae897c4acd4eaca76f3daf88f4159f **SHA-256 :** 44281718cfeb81103e4b28138c10db590e7ef7fa(**SHA-512 :** 38025bc346f4ce0ba20ab4a7afcf3696311b9900e **Size :** 0.104 Kilobytes.
C:\Program Files (X86)\Hohi\Selitopehohi.Bat	**Type :** data **MD5 :** ef1095dddbd9609aafe1093306d67ab6 **SHA-1 :** ca8cc6fe13d055d55ddf4f3839584870a6b8a2b0 **SHA-256 :** 85e6294a11bcae99b7a590069bc7ca9de8ed998 **SHA-512 :** 45c6b0a9c369b90d859c2d9ce94ab57d8b84e0cc **Size :** 0.979 Kilobytes.
C:\Program Files (X86)\Hohi\Nolika	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 05039c40abb926cedbb4d89945ed5fb3 **SHA-1 :** 3ac50bcab60eae08b8319a8aceea5873a35e1adb **SHA-256 :** 94eaf0ccee4c9781a28f947f1b1ab463242f5011a **SHA-512 :** 634cbfbb92249df62a3ba8d9408676d161bd205(**Size :** 0.697 Kilobytes.
C:\Program Files (X86)\Hohi\Fokufofefo.Exe	**Type :** data **MD5 :** 6b82e5449828055c7d90955e2b1de303 **SHA-1 :** 1d71d870a4ece8120bc5902d3d7a87fcfe9b86e5 **SHA-256 :** 8d7bd8373992262090c1e491b261da288af06c88 **SHA-512 :** 673df6898941e447536e8cda55740c1e4bf8e9e5 **Size :** 0.524 Kilobytes.
C:\Program Files (X86)\Hohi\Pufopereme.M3u	**Type :** data **MD5 :** 81c8f8b39da4e9d0a1529a26f3274767 **SHA-1 :** 826d2641b9ea802513ce65d6765baca5f18c6689 **SHA-256 :** b48ded431ae6c1eeef5a1acc5b9d04dc79de62b8 **SHA-512 :** 32528f47fddc0c3ab89ee604e99505bb3ca92ea8 **Size :** 0.863 Kilobytes.
C:\Program Files (X86)\Hohi\Fomen.Bat	**Type :** data **MD5 :** 51e9b41aa8eb7f87b6b2bf605b147cc3 **SHA-1 :** 278feeda7dadbd749cab18e91795f936c392b692 **SHA-256 :** 1395e9ef861c0cbac6be56f7490a66ffbdba4eb9d **SHA-512 :** b433b2a2137298b77f24b627cf376bf975bb10e2 **Size :** 0.886 Kilobytes.
C:\Program Files (X86)\Hohi\Fakahicedah.Mp3	**Type :** data **MD5 :** 9b99cdb7d7f2346f55f062315c7f7ac5 **SHA-1 :** aafe4f53267afb187f6336c7361ce2235776f8cf **SHA-256 :** a0b33b696215f4ea3cf9f18ba60a26b679afa948e **SHA-512 :** b623fc8330b47b4c6f3fbe69c34d9be1da5f54d4c **Size :** 1.006 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Hohi\Lerih.K	**Type :** data **MD5 :** dab840d8efdbf25749aea6578e7fba78 **SHA-1 :** d0778bd4b678aad804000b69e5dcf65fa45e5876 **SHA-256 :** ab23e4ec1b0fa6c5374aef6dc68d38e9aa57eec6 **SHA-512 :** fe14a20beabe6e1cda3f6c88874154761fa9a8e4 **Size :** 1.064 Kilobytes.
C:\Program Files (X86)\Hohi\Pegusogam.M3u	**Type :** data **MD5 :** e5aed82e7922f124cf84547e81acaf58 **SHA-1 :** 808abf9e75c98f8810fd7bd6096efe659c5f3d26 **SHA-256 :** 02db768111e666c1c263e73f5b63199c66ebfa06 **SHA-512 :** 39fee7e9b6cb8146321677926632893 5e15e22c5 **Size :** 0.327 Kilobytes.
C:\Program Files (X86)\Hohi\Fasedoc.Hi	**Type :** DOS executable (COM) **MD5 :** 8fc2a350464596b412b352ad30cab4ca **SHA-1 :** 77086bb0c0a403ba7fdf1fa37bd560499dd9e4ca **SHA-256 :** 6226a65dd2390852f67d010168a13b4e91b4165 **SHA-512 :** b778dd8a2ff593232db95dcfe6637e3892133428 **Size :** 0.317 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	advanced-rar-repair-programas-gratis-net.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	55bfa6aa04a16a892acdb2cc410192ab21e886a3
MD5:	178b4faf2ee615e96d2b27d0cd94794b
First Seen Date:	2017-04-15 02:04:20.375291 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2017-04-15 02:04:20.375291 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	8
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	
FileVersion	2.7.3.1
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Fudom
ProductVersion	1.6.9
FileDescription	Fudom Setup
Translation	0x0000 0x04b0
Entry Point	0x40a5f8 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	1271024
Sha256	2cf30c65450f9e7ee67662d5f1d4f8628f65d7fcc31169d4875d0575ff269444
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x9d30	0x9e00	6.641238	-
DATA	0xb000	0x250	0x400	2.754717	-
BSS	0xc000	0xe90	0x0	0.000000[SUSPICIOUS]	-
.idata	0xd000	0x950	0xa00	4.430733	-
.tls	0xe000	0x8	0x0	0.000000[SUSPICIOUS]	-
.rdata	0xf000	0x18	0x200	0.204488[SUSPICIOUS]	-
.reloc	0x10000	0x8c4	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x11000	0x2c00	0x2c00	4.573813	-

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc

    - LocalFree
    - LocalAlloc
    - WideCharToMultiByte
    - TlsSetValue
    - TlsGetValue
    - MultiByteToWideChar
    - GetModuleHandleA
    - GetLastError
    - GetCommandLineA
    - WriteFile
    - SetFilePointer
    - SetEndOfFile
    - RtlUnwind
    - ReadFile
    - RaiseException
    - GetStdHandle
    - GetFileSize
    - GetSystemTime
    - GetFileType
    - ExitProcess
    - CreateFileA
    - CloseHandle
- user32.dll
    - MessageBoxA
- oleaut32.dll
    - VariantChangeTypeEx
    - VariantCopyInd
    - VariantClear
    - SysStringLen
    - SysAllocStringLen
- advapi32.dll
    - RegQueryValueExA
    - RegOpenKeyExA
    - RegCloseKey
    - OpenProcessToken
    - LookupPrivilegeValueA
- kernel32.dll
    - WriteFile
    - VirtualQuery
    - VirtualProtect
    - VirtualFree
    - VirtualAlloc
    - Sleep
    - SizeofResource
    - SetLastError
    - SetFilePointer
    - SetErrorMode
    - SetEndOfFile
    - RemoveDirectoryA
    - ReadFile
    - LockResource
    - LoadResource
    - LoadLibraryA
    - IsDBCSLeadByte
    - GetWindowsDirectoryA
    - GetVersionExA
    - GetUserDefaultLangID
    - GetSystemInfo
    - GetSystemDefaultLCID
    - GetProcAddress
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLocaleInfoA
    - GetLastError
    - GetFullPathNameA
    - GetFileSize
    - GetFileAttributesA
    - GetExitCodeProcess
    - GetEnvironmentVariableA
    - GetCurrentProcess
    - GetCommandLineA
    - GetACP
    - InterlockedExchange
    - FormatMessageA
    - FindResourceA

    - DeleteFileA
    - CreateProcessA
    - CreateFileA
    - CreateDirectoryA
    - CloseHandle
- user32.dll
    - TranslateMessage
    - SetWindowLongA
    - PeekMessageA
    - MsgWaitForMultipleObjects
    - MessageBoxA
    - LoadStringA
    - ExitWindowsEx
    - DispatchMessageA
    - DestroyWindow
    - CreateWindowExA
    - CallWindowProcA
    - CharPrevA
- comctl32.dll
    - InitCommonControls
- advapi32.dll
    - AdjustTokenPrivileges

PE Resources

RT_ICON
RT_STRING
RT_RCDATA
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Success ✔

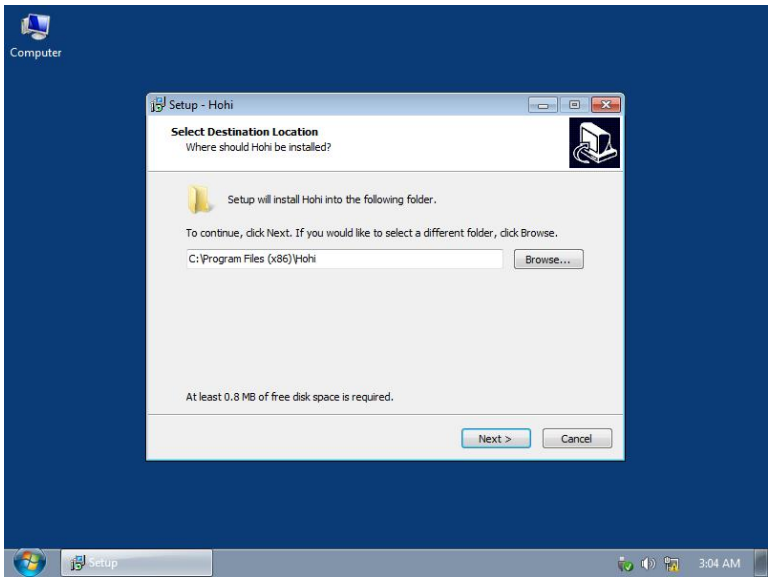
[+] MediaProgramas SL	
Status	NoError ✔
Start Date	2017-01-18 00:00:00+00:00
End Date	2018-03-19 23:59:59+00:00
Sha256	a64bd70266bfd5bb5a9fe73235ead93192f2ef9b25395094dca760bb7125ca95
Serial	3737FD96326D2D02DBC5EDD147523773
Subject Key Identifier	f6 b7 8b 9d 0a 53 cc 40 e9 86 16 81 42 7b e5 8c 63 a5 f2 51
Issuer Name	thawte SHA256 Code Signing CA
Issuer Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Crl link	http://tl.symcb.com/tl.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

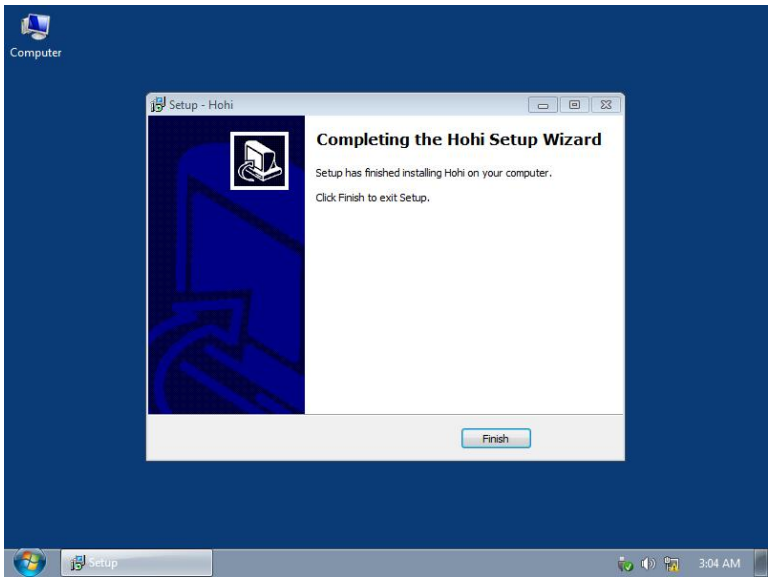
[+] thawte SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 00:00:00+00:00
End Date	2023-12-09 23:59:59+00:00
Sha256	d542ad03871f39ed7a47a057892a67f6d76b973134a8a129d2ba1ace821de2e4
Serial	71A0B73695DDB1AFC23B2B9A18EE54CB
Subject Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Crl link	http://t1.symcb.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

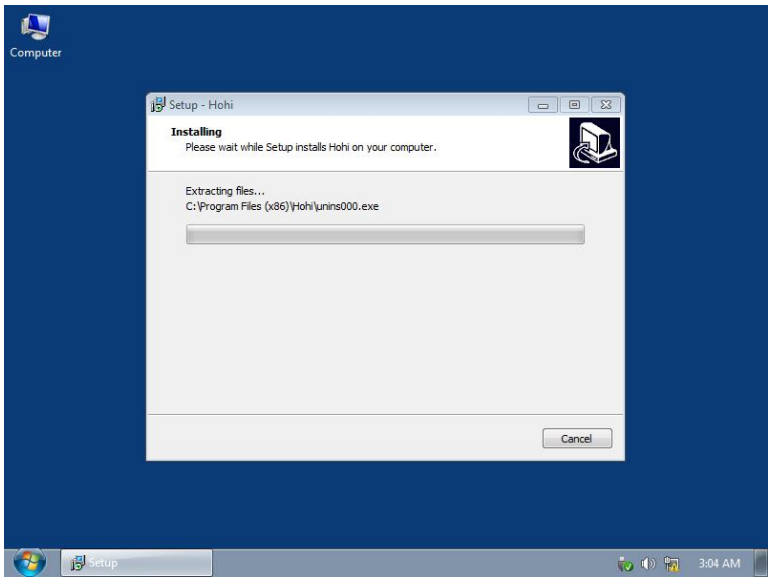
[+] thawte Primary Root CA	
Status	NoError ✔
Start Date	2006-11-17 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

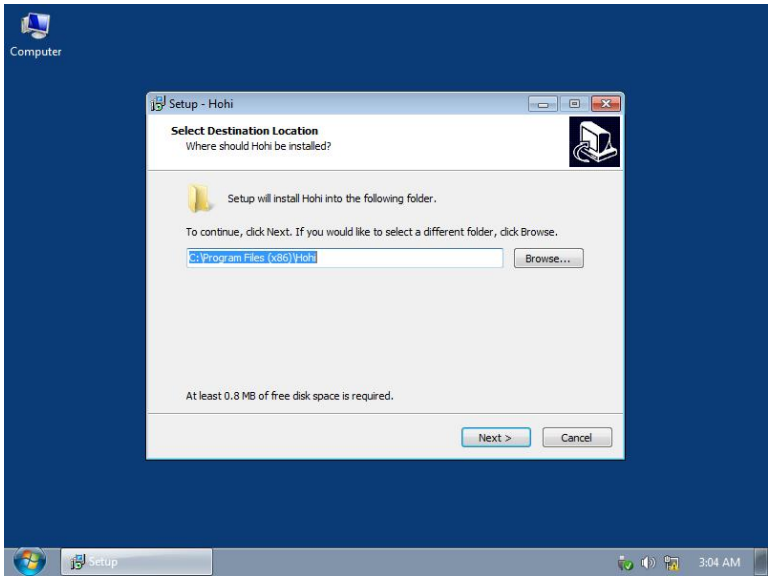
SCREENSHOTS


Computer
3:04 AM

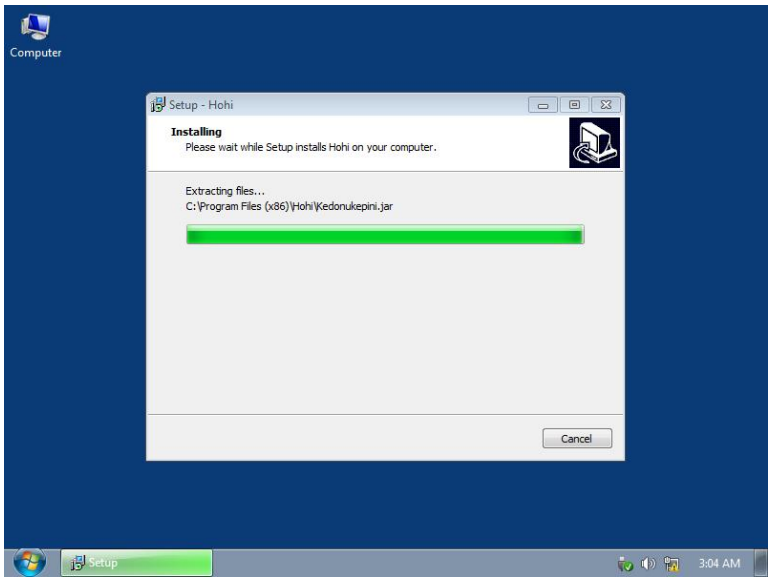

Computer
Setup - Hohi
Select Destination Location
Where should Hohi be installed?
Setup will install Hohi into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Hohi
Browse...
At least 0.8 MB of free disk space is required.
Next >
Cancel
Setup
3:04 AM

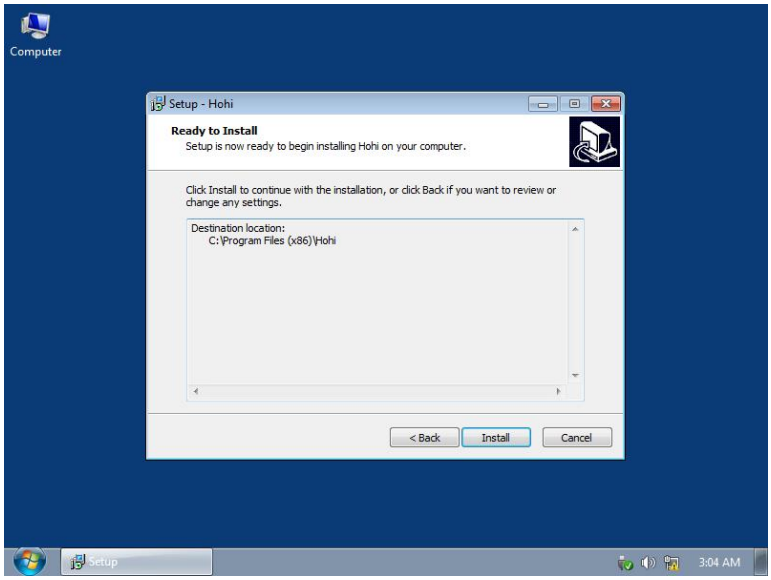

Computer
Setup - Hohi
Completing the Hohi Setup Wizard
Setup has finished installing Hohi on your computer.
Click Finish to exit Setup.
Finish
Setup
3:04 AM


Computer
Setup - Hohi
Installing
Please wait while Setup installs Hohi on your computer.
Extracting files...
C:\Program Files (x86)\Hohi\unins000.exe
Cancel
Setup
3:04 AM


Computer
Setup - Hohi
Select Destination Location
Where should Hohi be installed?
Setup will install Hohi into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Hohi
Browse...
At least 0.8 MB of free disk space is required.
Next >
Cancel
Setup
3:04 AM


Computer
3:04 AM


Computer
Setup - Hohi
Installing
Please wait while Setup installs Hohi on your computer.
Extracting files...
C:\Program Files (x86)\Hohi\Kedonukepini.jar
Cancel
Setup
3:04 AM


Computer
Setup - Hohi
Ready to Install
Setup is now ready to begin installing Hohi on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\Hohi
< Back
Install
Cancel
Setup
3:04 AM