Corona.sh4

Is DLL | Packer | Anti Debug | Anti VM | Signed | XOR

MalFamily: Linux **MalScore: 100**

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, not stripped
File size:	55.02 KB (56338 bytes)
Compile time:	0000-00-00 00:00:00
MD5:	ad0093283b1477efe7a834d20e054bd0
SHA1:	b255c0c56d1ad4d09ee7b3ab285adb9252ec15ca
Submitted:	2021-01-28 23:57:05

URL(s) file hosting

http://91.212.150.241/Corona.sh4

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

2 Behaviors detected by system signatures

Dynamic (imported) function loading detected

- DynamicLoader: SHELL32.dll/OpenAs_RunDLLW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: SHELL32.dll/
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey

- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: comctl32.dll/InitCommonControlsEx
- DynamicLoader: uxtheme.dll/EnableThemeDialogTexture
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/GetThemeBool
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: uxtheme.dll/BufferedPaintInit
- DynamicLoader: uxtheme.dll/BufferedPaintRenderAnimation
- DynamicLoader: uxtheme.dll/BeginBufferedAnimation
- DynamicLoader: uxtheme.dll/IsThemeBackgroundPartiallyTransparent
- DynamicLoader: uxtheme.dll/DrawThemeParentBackground
- DynamicLoader: uxtheme.dll/GetThemePartSize
- DynamicLoader: uxtheme.dll/DrawThemeBackground
- DynamicLoader: uxtheme.dll/GetThemeBackgroundContentRect
- DynamicLoader: uxtheme.dll/DrawThemeText
- DynamicLoader: uxtheme.dll/EndBufferedAnimation
- DynamicLoader: uxtheme.dll/GetThemeTransitionDuration
- DynamicLoader: OLEAUT32.dll/SysAllocString
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: OLEAUT32.dll/SysFreeString

SetUnhandledExceptionFilter detected (possible anti-debug)