putty.jpg

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

MalFamily: Linux **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	564.00 KB (577536 bytes)
Compile time:	1976-01-24 03:01:35
MD5:	c0537fd9e1eae23fb5cc659c8b08ed10
SHA1:	71652a6fedb14df02907e945ac31b73274862a2b
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-10-30 20:39:04

URL(s) file hosting

http://euromouldings.cf/putty.jpg

Antivirus Report

Report date	Detection Ratio	Permalink
2018-10-30 14:04:15	22/68	

Import library

mscoree.dll

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)