文件检测评级：

未发现风险

文件名称： 文本编辑器1.0.zip

基本信息

文件名称：	文本编辑器1.0.zip
MD5：	69836073391e81e0b1076ae3284cd31b
文件类型：	zip
上传时间：	2018-02-19 15:39:56
出品公司：	N/A
版本：	N/A
壳或编译器信息：	N/A
子文件信息：	长风 文本编辑器.exe / a8d9f2cd5f3e1cfedb34c7def06124be / EXE
	长风 文本编辑器.pdb / 25cfb81cd06d1ec6d54d212cf33a21f5 / Unknown
	长风 文本编辑器.vshost.exe / c243735fc91d039eba1f7d1b84e26037 / EXE
	长风 文本编辑器.xml / 604401a444de0536b2bb45e420230fa8 / Unknown

关键行为

行为描述：直接获取CPU时钟

详情信息： EAX = 0x81f0e56f, EDX = 0x00000085

EAX = 0x81f0e5bb, EDX = 0x00000085

EAX = 0x872bb474, EDX = 0x00000085

EAX = 0x872bb4c0, EDX = 0x00000085

EAX = 0x872bb50c, EDX = 0x00000085

EAX = 0x872bb558, EDX = 0x00000085

EAX = 0x8f198341, EDX = 0x00000085

EAX = 0x8f19838d, EDX = 0x00000085

EAX = 0xb158898a, EDX = 0x00000085

EAX = 0xb15889d6, EDX = 0x00000085

行为描述：获取TickCount值

详情信息： TickCount = 224879, SleepMilliseconds = 20.

TickCount = 224895, SleepMilliseconds = 20.

TickCount = 284875, SleepMilliseconds = 60000.

文件行为

行为描述：覆盖已有文件

详情信息： C:\\Users\\Administrator\\AppData\\Local\\GDIPFONTCACHEV1.DAT

行为描述：查找文件

详情信息： FileName = C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\mscoreei.dll

FileName = C:\\Windows\\Microsoft.NET\\Framework*

FileName = C:\\Windows

FileName = C:\\Windows\\WinSxS

FileName = C:\\Windows\\WinSxS\\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\\MSVCR80.dll

FileName = C:\\Windows\\assembly\\GAC_32\\mscorlib\\2.0.0.0__b77a5c561934e089\\mscorlib.INI

FileName = C:\\Users

FileName = C:\\Users\\Administrator\\AppData

FileName = C:\\Users\\Administrator\\AppData\\Local

FileName = C:\\Users\\Administrator\\AppData\\Local\\Temp

FileName = C:\\Users\\Administrator\\AppData\\Local\\%temp%

FileName = C:\\Users\\Administrator\\AppData\\Local\\%temp%\\b70c.exe_7zdump\\长风文本编辑器.exe

FileName = C:\\Users\\Administrator

FileName = C:\\Users\\Administrator\\AppData\\Local\\%temp%\\b70c.exe_7zdump

FileName = C:\\Users\\Administrator\\AppData\\Local\\%temp%\\b70c.exe_7zdump\\长风文本编辑器.INI

注册表行为

行为描述：修改注册表

详情信息： \\REGISTRY\\USER\\S-*\\Software\\Microsoft\\GDIPlus\\FontCachePath

其他行为

行为描述：检测自身是否被调试

详情信息： IsDebuggerPresent

行为描述：创建事件对象

详情信息： EventName = Global\\CorDBIPCSetupSyncEvent_3688

行为描述：打开互斥体

详情信息： Global\\CLR_CASOFF_MUTEX
Local\\MSCTF.Asm.MutexDefault1

行为描述：打开事件

详情信息： Global\\CLR_PerfMon_StartEnumEvent
HookSwitchHookEnabledEvent
\\KernelObjects\\LowMemoryCondition
Local\\MSCTF.CtfActivated.Default1
Local\\MSCTF.AsmCacheReady.Default1
MSFT.VSA.COM.DISABLE.3688
MSFT.VSA.IEC.STATUS.6c736db0

行为描述：获取TickCount值

详情信息： TickCount = 224879, SleepMilliseconds = 20.
TickCount = 224895, SleepMilliseconds = 20.
TickCount = 284875, SleepMilliseconds = 60000.

行为描述：窗口信息

详情信息： Pid = 3688, Hwnd=0x101bc, Text = StatusStrip1, ClassName =
WindowsForms10.Window.8.app.0.378734a.
Pid = 3688, Hwnd=0x101be, Text = ToolStrip1, ClassName =
WindowsForms10.Window.8.app.0.378734a.
Pid = 3688, Hwnd=0x101c0, Text = MenuStrip1, ClassName =
WindowsForms10.Window.8.app.0.378734a.
Pid = 3688, Hwnd=0x401b8, Text = 长风 文本编辑器, ClassName =
WindowsForms10.Window.8.app.0.378734a.

行为描述：调用Sleep函数

详情信息： [1]: MilliSeconds = -1.
[2]: MilliSeconds = 20.

[3]: MilliSeconds = 20.

行为描述：直接获取CPU时钟

详情信息： EAX = 0x81f0e56f, EDX = 0x00000085

EAX = 0x81f0e5bb, EDX = 0x00000085

EAX = 0x872bb474, EDX = 0x00000085

EAX = 0x872bb4c0, EDX = 0x00000085

EAX = 0x872bb50c, EDX = 0x00000085

EAX = 0x872bb558, EDX = 0x00000085

EAX = 0x8f198341, EDX = 0x00000085

EAX = 0x8f19838d, EDX = 0x00000085

EAX = 0xb158898a, EDX = 0x00000085

EAX = 0xb15889d6, EDX = 0x00000085

运行截图