文件检测评级：

未发现风险

文件名称： 沉寂的文件加解密工具.exe

基本信息

文件名称：	沉寂的文件加解密工具.exe
MD5：	173c420215e91e832ce2ee7cdca5fd04
文件类型：	EXE
上传时间：	2017-01-20 17:26:09
出品公司：	繁华中的沉寂
版本：	1.0.0.0---1.0.0.0
壳或编译器信息：	COMPILER:Elan

关键行为

行为描述：获取窗口截图信息

详情信息： Foreground window Info: HWND = 0x00000000, DC = 0x4c01051e.

Foreground window Info: HWND = 0x00000000, DC = 0x1a01067a.

Foreground window Info: HWND = 0x00000000, DC = 0x4601069b.

Foreground window Info: HWND = 0x00000000, DC = 0x4901069b.

进程行为

行为描述：创建本地线程

详情信息： TargetProcess: %temp%****.exe, InheritedFromPID = 1944, ProcessID = 780, ThreadID = 1204, StartAddress = 4AEA7456, Parameter = 00000000

文件行为

行为描述：覆盖已有文件

详情信息： C:\\Documents and Settings\\Administrator\\Local Settings\\Application Data\\GDIPFONTCACHEV1.DAT

其他行为

行为描述：创建互斥体

详情信息： CTF.LBES.MutexDefaultS-*

CTF.Compart.MutexDefaultS-*

CTF.Asm.MutexDefaultS-*

CTF.Layouts.MutexDefaultS-*

CTF.TMD.MutexDefaultS-*

CTF.TimListCache.FMPDefaultS-*MUTEX.DefaultS-*

MSCTF.Shared.MUTEX.ELH

MSCTF.Shared.MUTEX.AHF

行为描述：创建事件对象

详情信息： EventName = DINPUTWINMM

EventName = MSCTF.SendReceive.Event.AHF.IC

EventName = MSCTF.SendReceiveConection.Event.AHF.IC

行为描述：查找指定窗口

详情信息： NtUserFindWindowEx: [Class,Window] = [Shell_TrayWnd,]

NtUserFindWindowEx: [Class,Window] = [CicLoaderWndClass,]

NtUserFindWindowEx: [Class,Window] = [OleMainThreadWndClass,]

行为描述：打开事件

详情信息： HookSwitchHookEnabledEvent

CTF.ThreadMIConnectionEvent.000007B4.00000000.00000052

CTF.ThreadMarshalInterfaceEvent.000007B4.00000000.00000052

MSCTF.SendReceiveConection.Event.ELH.IC

MSCTF.SendReceive.Event.ELH.IC

行为描述：窗口信息

详情信息： Pid = 780, Hwnd=0xf03c8, Text = 作者信息, ClassName = _EL_HyperLinker.

Pid = 780, Hwnd=0xb03ba, Text = 小贴士：直接拖动文件到窗口也可以哦, ClassName = _EL_Label.

Pid = 780, Hwnd=0x40394, Text = RC4算法, ClassName = Button(RadioButton).

Pid = 780, Hwnd=0x6037e, Text = 请选择加密算法：, ClassName = _EL_Label.

Pid = 780, Hwnd=0x403ca, Text = DES算法, ClassName = Button(RadioButton).

Pid = 780, Hwnd=0xc038a, Text = 请输入密码：, ClassName = _EL_Label.

Pid = 780, Hwnd=0x303dc, Text = 请选择您要加/解密的文件：, ClassName = _EL_Label.

Pid = 780, Hwnd=0x1f02fe, Text = 123456, ClassName = Edit.

Pid = 780, Hwnd=0x110320, Text = 123456, ClassName = Edit.

行为描述：获取窗口截图信息

详情信息： Foreground window Info: HWND = 0x00000000, DC = 0x4c01051e.

Foreground window Info: HWND = 0x00000000, DC = 0x1a01067a.

Foreground window Info: HWND = 0x00000000, DC = 0x4601069b.

Foreground window Info: HWND = 0x00000000, DC = 0x4901069b.

行为描述：隐藏指定窗口

详情信息： [Window,Class] = [,WindowEx]

[Window,Class] = [,ButtonEx]

[Window,Class] = [,_EL_CommonDlg]

[Window,Class] = [,Afx:400000:b:10011:1900010:0]

[Window,Class] = [,ChoiceboxEx]

行为描述：打开互斥体

详情信息： ShimCacheMutex

运行截图