文件检测评级：

# 未发现风险

文件名称： Duplicate Photo Finder Plus.exe

## 基本信息

| | |
|---|---|
| 文件名称： | Duplicate Photo Finder Plus.exe |
| MD5： | 63d7f9b72187536813ffa5a6b302310a |
| 文件类型： | EXE |
| 上传时间： | 2020-09-11 09:13:33 |
| 出品公司： | TriSun Software Limited |
| 版本： | 12.0.40.0---12.0.040 |
| 壳或编译器信息： | COMPILER:Microsoft Visual C# / Basic .NET |

## 关键行为

行为描述：跨进程写入数据

详情信息： TargetProcess = C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\dw20.exe, WriteAddress = 0x00150000, Size = 0x00000020 TargetPID = 0x00000854
TargetProcess = C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\dw20.exe, WriteAddress = 0x00150020, Size = 0x00000034 TargetPID = 0x00000854
TargetProcess = C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\dw20.exe, WriteAddress = 0x7ffd6238, Size = 0x00000004 TargetPID = 0x00000854

行为描述：直接获取CPU时钟

详情信息： EAX = 0x0058b09a, EDX = 0x0000039a
EAX = 0x05beaf46, EDX = 0x0000039a
EAX = 0x27fdb543, EDX = 0x0000039a
EAX = 0x32735269, EDX = 0x0000039a
EAX = 0x327352b5, EDX = 0x0000039a
EAX = 0x35265231, EDX = 0x0000039a
EAX = 0x3526527d, EDX = 0x0000039a
EAX = 0x352652c9, EDX = 0x0000039a
EAX = 0x35265315, EDX = 0x0000039a
EAX = 0x35265361, EDX = 0x0000039a

行为描述：获取TickCount值

详情信息： TickCount = 1101311, SleepMilliseconds = -1.

TickCount = 1101358, SleepMilliseconds = -1.

TickCount = 1130999, SleepMilliseconds = -1.

TickCount = 1160999, SleepMilliseconds = -1.

# 进程行为

- 创建进程
- 跨进程写入数据

# 文件行为

- 查找文件

# 其他行为

- 检测自身是否被调试
- 创建互斥体
- 创建事件对象
- 打开互斥体
- 打开事件
- 获取TickCount值
- 枚举窗口
- 调用Sleep函数
- 隐藏指定窗口
- 直接获取CPU时钟