|  |  |  |  |
| --- | --- | --- | --- |
| V1.0 | 2018年7月10日 | 开始试用 | 刘强 |
| V1.1 | 2018年7月12日 | 增加UiPath使用经验 | 刘强 |
| V1.2 | 2018年7月15日 | 增加UiPath使用经验 | 刘强 |
| V2.0 | 2018年7月19日 | 修改RAT工作目录，添加output转存日期，工程模块化 | 刘强 |

1. 测试环境准备
   1. Windows 7，~~DLL检查器，~~关闭UAC，防火墙，360，更新powershell执行策略。进入powershell输入：set-executionpolicy remotesigned。输入法换成英文。
   2. 更新` tools\apps\update\_address\_map.bat`的代码，需要更新的有：WinRAR的地址。
   3. 更新Collector软件。（按需）
   4. 运行` tools\apps\update\_address\_map.bat`更新Collector的address map（保证网络连接，1~2分钟）。成功如图 1所示。

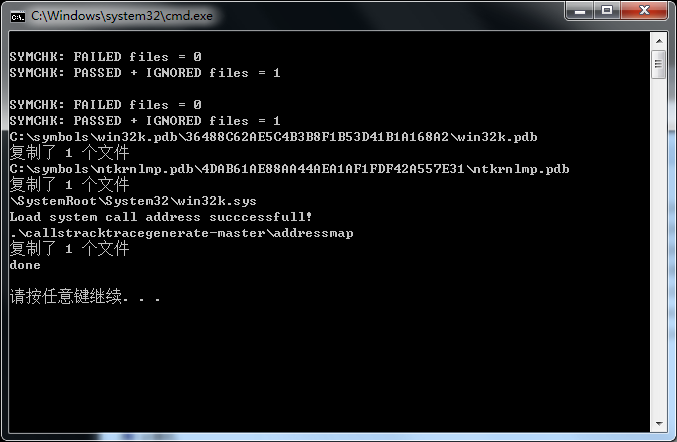


图 1

* 1. 安装Python2.7。
  2. 安装UiPath Studio（需要连网，按提示输入邮箱即可，如cyruscyliu@gmail.com）。打开UiPath Studio找到包管理器，如图 2所示。打开包管理器，在Available中搜索UiPath.Script.Activities，点击install安装。

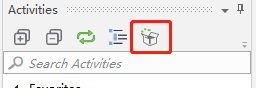


图 2

1. 配置RAT（每添加一个新的RAT）
   1. 按下表所示路径和文件名放置RAT

|  |
| --- |
| c:\tools\rats\rat\_name\_v[[1]](#footnote-1)\server.exe（需要提前生成） |
| c:\tools\rats\rat\_name\_v\rat\_name.exe |

1. 配置UiPath工程生成器（每添加一个新的RAT）
   1. configuration.py

|  |  |
| --- | --- |
| ROOT：“c:\\tools” | 工具包路径 |
| COLLECTOR\_NAME：'ETWDataCollectorRedesigned.exe' | Collector名（按需[[2]](#footnote-2)） |
| LINE\_NUMBER：12 | （按需[[3]](#footnote-3)） |

1. 生成UiPath工程（每添加一个新的RAT）

|  |
| --- |
| c:\python2.7\python.exe uipath\_project\_render.py c:\tools\rat\_name\_v\rat\_name.exe |

示例见tools\render\_sample.bat。

生成的工程文件是c:\tools\uipath\_projects\rat\_name\rat\_name.xaml，如图 3所示。

python.exe的路径可能报错，python一般在c:\python27下，请自行察看。

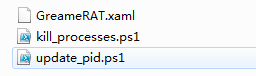


图 3

1. 打开UiPath Studio，选择Open，打开生成的工程文件（xaml）。打开该工程，可见测试框架，如图 4所示。

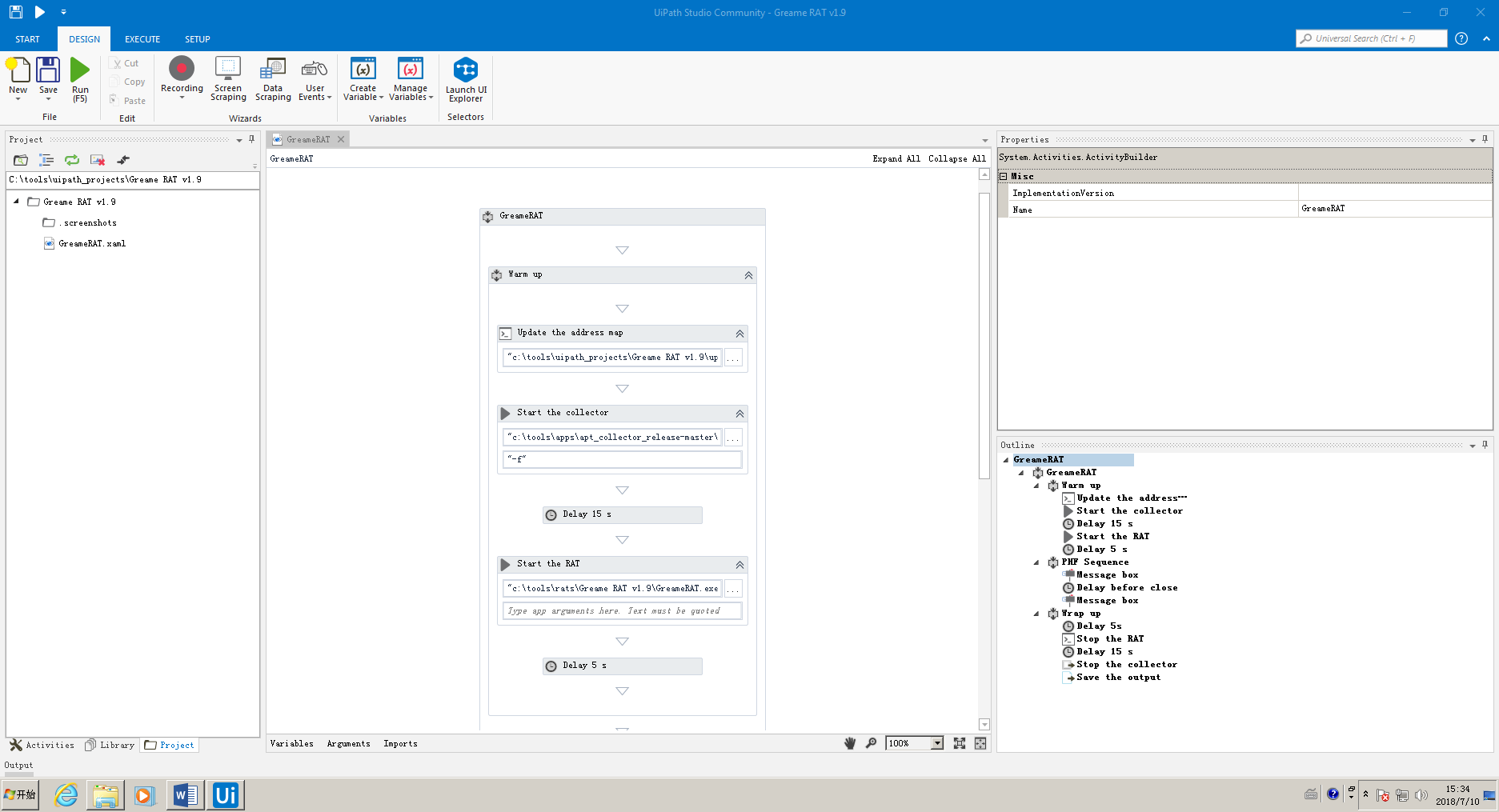


图 4

1. 在PHF Sequence内录制PHF。
   1. 任务要求
      1. 录制5个PHF，分别是Remote Desktop、Remote Audio、Remote Shell、Download & Execution and KeyLogger。
      2. 每录制一个PHF都需要持续一定时间，如60s，以保证捕捉到相应的行为，将数据文件重命名移到相应位置。整个RAT下来，需要5~6分钟。
      3. 录制后的调整过程中，请注意修改output的文件名。
   2. 相关经验
      1. 先录好一个，能用再复制。可以使用多个大Sequence，提高调试效率。
      2. 当RAT自动弹网页、资源管理器的时候，请在Start the RAT后先使用Set Focus。
      3. “点击鼠标右键”录制成“点击”鼠标左键，而后利用UiPath Studio调整成右键。
      4. 利用F2暂停录制，点击鼠标右键弹出相关菜单。
      5. 录制按钮时，请先将鼠标放置到按钮上，保证录制过程中，程序能正常执行。比如，录制“关闭窗口”时，按F2，将鼠标移至右上角，关闭按钮会发生颜色变化，录制时，点击鼠标左键，该动作被录制的同时，该窗口也应该被关闭。
      6. 点击动作录制不成功（执行不成功或者录成了Select Item），需要重新录制该动作。首先，使用录制面板上的“录制点击功能”，如图 5所示。再使用Click Image功能。再使用Click OCR Image功能。一般，录制面板即可解决问题。

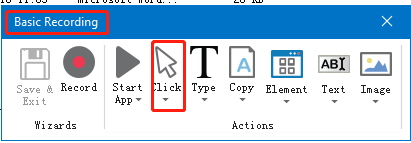
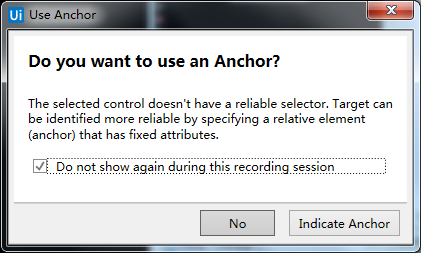


图 5

* + 1. 重复操作录制一次，复制以下即可。粘贴时，选中活动之间的倒三角。
    2. 运行时可利用disable功能就行部分调试
    3. 运行时桌面窗口不要放太多
  1. 一些问题
     1. 弹出Do you want to use an Anchor? 选中Do not show…，点击No。当前动作已经被录制。



1. 带版本号的RAT名字 [↑](#footnote-ref-1)
2. Collector更新后主程序的名字有时候会变换，请做好区分。 [↑](#footnote-ref-2)
3. Collector更新后，需要确定`output\_whitelist\_processid `的行号，并将行号减1赋值给LINE\_NUMBER。 [↑](#footnote-ref-3)