

工控网络流量沙箱检测系统

同往、與梓烽、办埃畚、土梓博

联系方式：向佳、18420204127、yujia@iscas.ac.cn

等特点对现有沙箱方案构成挑战。工控网络流量沙箱检测系统直接针对工控设备间“交互流量”进行沙箱检测，通过网络流量重构和重放，对流量驱动下的工控软件行为进行攻击检测，该系统具备数据包乱序修正、数据去冗余和还原等流量重构能力，实现了从“文件沙箱”升级到“流量沙箱”



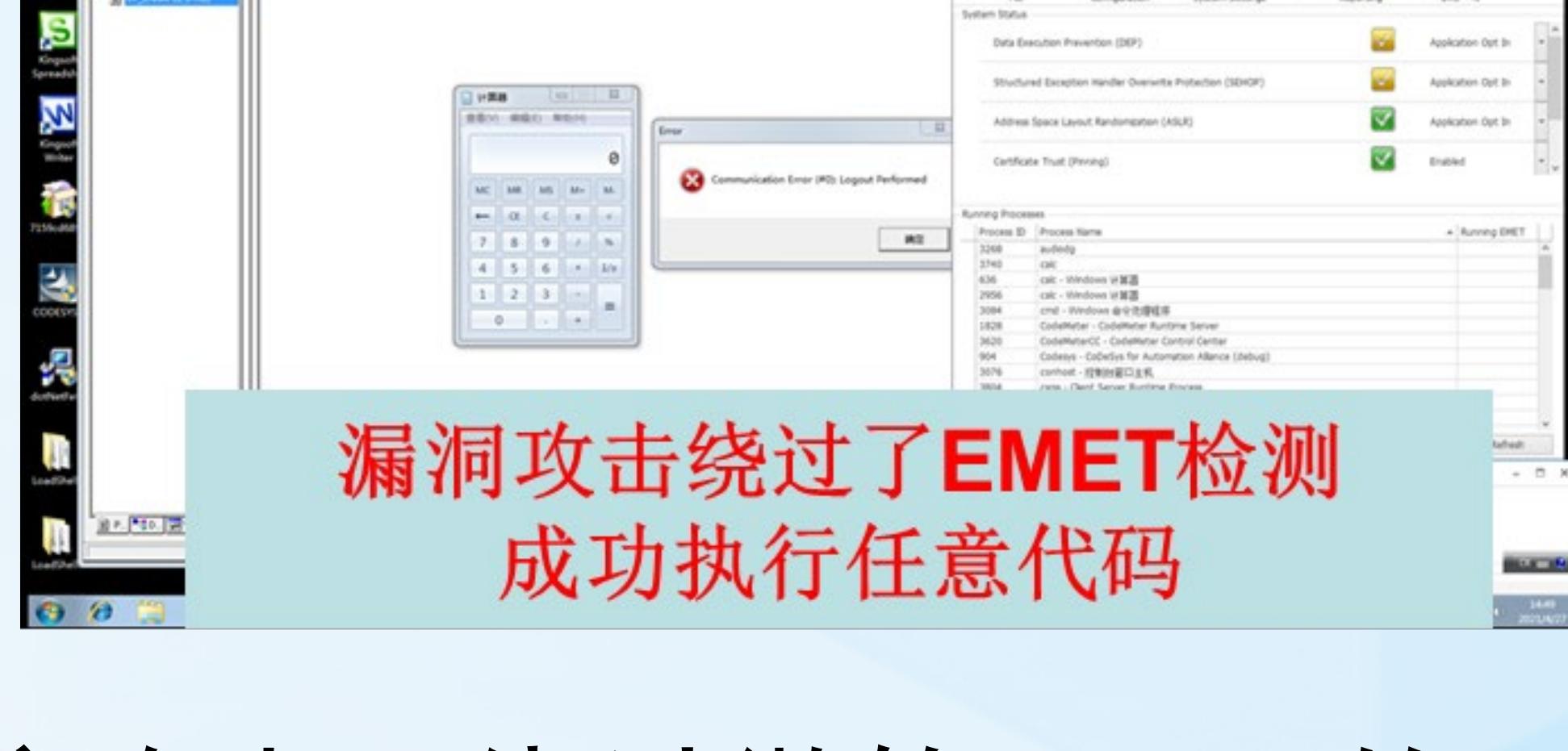
门子Step7

- 支持47类对抗样本的检测，与谷歌Virus Total 平台部署的同类沙箱相比，对抗能力显著提升

应用

- # ■ 中标某部车载安全设备采购项目

动态行为类目	查看详细结果数据	异常代码片段
+	行为类别	行为等级
进程开始执行	普通	被 (1256) 创建的进程开始执行



发送网络数据		普通	向本机发送网络数据
接收网络数据包		高危	接收来自 192.168.4.10: 35354 的数据包
发送网络数据包		高危	向 192.168.4.10: 35354 (Unknown Host) 发送网络数据
检测调试环境		普通	检测调试环境, 避免分析与查杀
+ 加载模块		普通	加载模块 HarddiskVolume1\WINDOWS\system32\faultrep.dll

[高危]	向 192.168.4.10: 35354 (Unknown Host) 发送网络数据
[普通]	检测调试环境, 逃避分析与查杀
[普通]	加载模块 HarddiskVolume1\WINDOWS\system32\faultrep.dll
[敏感]	读取文件 HarddiskVolume1\WINDOWS\system32\cmd.exe
 [高危]	读取 cmd.exe 进程中的数据, 窃取信息