2016 年 12 月 1 日，星期四

FIRST 项目：共享知识，加速分析

FIRST 项目由 Angel M. Villegas 领导。作者：Holger Unterbrink。

Talos 很高兴地宣布，正式发布函数识别和恢复签名工具 (FIRST)。函数识别和恢复签名工具是一个开源框架，允许分享关于 IDA Pro 可以分析的文件类型所用类似函数的知识。其目的是为信息安全分析员和逆向工程师打造一个促进信息共享的社区。

FIRST 背后的主要理念是通过使用操作码散列处理、助记符散列处理、位置敏感散列处理等方法来保留工程师对某些函数（名称、原型、注释等）的分析。该框架可以集中收集和存储这些签名，然后通过 API/插件将它们提供给社区。其目标是提供类似函数的快速查找（见图 A），以避免花费时间分析之前在其他样本中或由其他工程师分析过的函数。

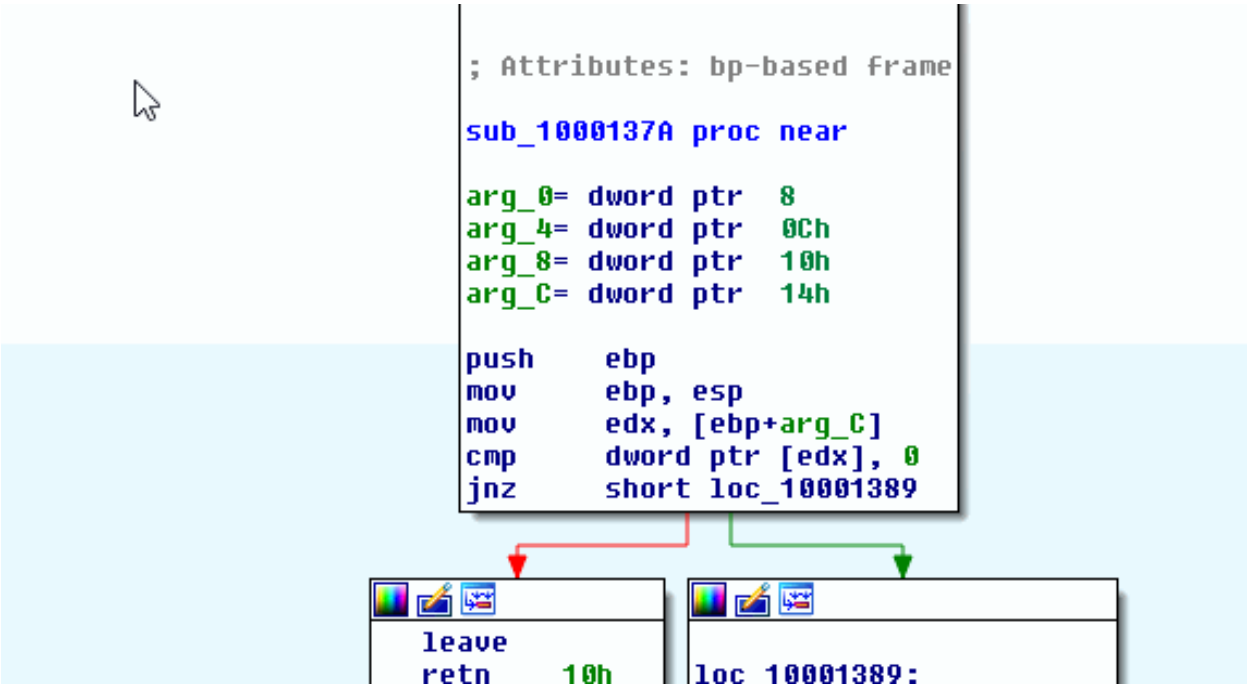

图 A

例如，西班牙的一名研究人员分析了一个样本。他为分析的函数添加了注释并将信息上传到服务器。后来，加利福尼亚的一名研究人员遇到了该样本的一个变体，他查询 FIRST 服务器，以找到与已知二进制文件的相似性。他很幸运，有人已经对这些函数进行了分析，因此他不需要白费力气做重复工作，他可以使用在框架中找到的匹配结果，加速其分析。

对于客户端，我们提供一个具有以下功能的 IDA Python 插件：

- 添加注释（单个或多个函数）
- 检查注释（单个或所有函数）
- 更新应用的注释
- 查看应用的注释
- 查看注释历史记录
- 管理元数据
- 通过 IDA Python 为 FIRST 写脚本

此插件可以与公共 Talos FIRST 服务器（测试版）或与您自己的服务器实例一起使用。首先您可以在 FIRST 主页上注册 Talos 服务器的 API 密钥。

FIRST 框架架构由以下组件构成。

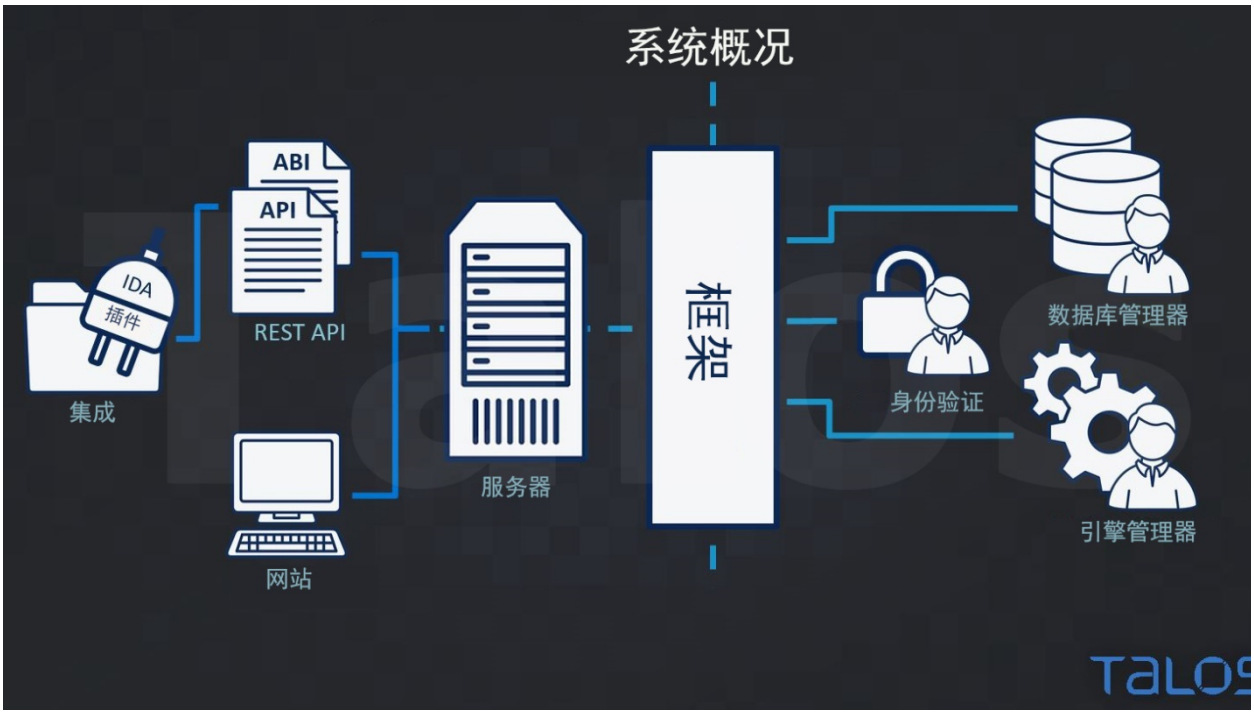

图 B

该框架提供一个 REST API，用于与客户端插件（如 IDA 插件）通信。此外，它还提供身份验证模型、数据库管理器和引擎管理器。数据库管理器提供集成所使用的 MongoDB 以外其他数据库（如 MySQL）的灵活性。引擎管理器管理并执行用于推导函数相似性的所有模块（称为“引擎”）。客户端插件/API/ABI 通过 REST API 与服务器交互。API/ABI 为开发人员提供了将 FIRST 纳入到其当前工作流程和工具的一种方法。

FIRST 已经并将在以下会议中进行介绍：

MALCON - 10 月 19 日波多黎各法哈多
PACSEC - 10 月 27 日日本东京
ZeroNights - 11 月 18 日俄罗斯莫斯科
Botconf - 12 月 1 日法国里昂

如需了解更多信息，请访问：

主页 - 注册和信息
http://first-plugin.us/

发布者：HOLGER UNTERBRINK；发布时间：12:30
标签：FIRST、IDA PRO、逆向工程、逆向