2017 年 11 月 22 日，星期三

Talos 凭借 Pyrebox 赢得第五届 Volatility 插件竞赛

Talos 凭借 Pyrebox 赢得今年的第 5 届 Volatility 插件竞赛。Volatility 是一款知名的用于分析操作系统内存的开源框架。该框架自 2007 年问世。在最初的 5 年中，他们推出了一个插件竞赛，旨在为 Volatility 寻找最具创新、最有趣和最有用的扩展。Pyrebox 是 Talos 开发的一款开源 Python 脚本化逆向工程沙盒。Pyrebox 基于 QEMU，其目的是通过从不同的角度提供动态分析和调试功能，来帮助实施逆向工程。在这种情况下，Pyrebox 能够与 Volatility 相互作用，从而收集所分析系统的内存的信息。

以下是该功能的一个代码片段：

```
[13] pyrebox(1f0)> vol pslist
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          
---------- -------------------- ------ ------ ------ -------- ------ ------ ----------------------------
0x817caa00 System                    4      0     72      150 ------      0                              
0x817d9b28 smss.exe                312      4      3       19 ------      0 2017-06-02 20:31:44 UTC+0000
0x81621020 csrss.exe               408    312     11      305      0      0 2017-06-02 20:31:45 UTC+0000
0x81620ad0 winlogon.exe            432    312     21      503      0      0 2017-06-02 20:31:46 UTC+0000
0x81609a00 services.exe            484    432     16      246      0      0 2017-06-02 20:31:48 UTC+0000
0x81604da0 lsass.exe               496    432     23      325      0      0 2017-06-02 20:31:48 UTC+0000
0x8179f020 svchost.exe             652    484     19      193      0      0 2017-06-02 20:32:00 UTC+0000
0x815f0998 svchost.exe             760    484      9      208      0      0 2017-06-02 20:32:29 UTC+0000
0x815ee488 svchost.exe            1064    484     58     1028      0      0 2017-06-02 20:33:55 UTC+0000
0x81605a08 svchost.exe            1084    484      5       58      0      0 2017-06-02 20:33:57 UTC+0000
0x8160e838 svchost.exe            1148    484     13      178      0      0 2017-06-02 20:34:03 UTC+0000
0x817427a0 explorer.exe           1156   1120     11      305      0      0 2017-06-02 20:34:04 UTC+0000
0x8161c880 spoolsv.exe            1304    484     15      122      0      0 2017-06-02 20:34:11 UTC+0000
0x81594298 alg.exe                1768    484      7      100      0      0 2017-06-02 20:34:30 UTC+0000
0x8158f020 wscntfy.exe            1796   1064      1       26      0      0 2017-06-02 20:34:33 UTC+0000
0x815eb020 wuauclt.exe             112   1064      8      176      0      0 2017-06-02 20:35:04 UTC+0000
```

您可以在博客文章中找到有关 Pyrebox 的更多信息。

Talos 支持可在 Github 资源库 中找到的许多开源项目。我们很高兴与更广泛的安全社区共享工具，并支持蓬勃发展的开源社区。除了项目的数量，第一名的位置进一步展示了我们开源项目的卓越性。

发布者：PAUL RASCAGNERES；发布时间：8:18 AM

标签：PYREBOX、TALOS、TALOS GITHUB、VOLATILITY