Technology Knowledge Base 2019-02

by bugnofree

Publish → 2019-02-01 Update → 2019-03-01

- 2019-02-11 @群成员.西莫

  推荐一个很好用的API监控工具：API Monitor

  监控相应的API并下断点，就可以在调用该API时停下来，看到相应的参数

  不设断点直接选中相应API，如果该API被调用，在右侧会有相应记录，也可以看到API被调用时的参数

  左下角会列出进程，可以双击或右键选择监控进程

  官网：http://www.rohitab.com/apimonitor

- 2019-02-15 https://osandamalith.com/2019/02...

  Linux Reverse Engineering CTFs for Beginners

- 2019-02-16 https://github.com/processhacker...

  A free, powerful, multi-purpose tool that helps you monitor system resources, debug software and detect malware.

- 2019-02-17 https://www.freebuf.com/vuls/195...

  邮件钓鱼攻击与溯源

  十分精彩, 膜拜大佬.

- 2019-02-18 https://erfur.github.io/down_the...

[EN] Down the Rabbit Hole - Part I: A Journey into the UEFI Land

- 2019-02-19 https://erfur.github.io/down_the...

  [EN] Down the Rabbit Hole - Part II: Analyzing an EFI Application with Radare2

- 2019-02-20 https://blog.perfect.blue/ROPing...

  ROP-ing on Aarch64 - The CTF Style

  - 来自 @vancir https://github.com/tanjiti/sec_p...

    爬取secwiki和xuanwu.github.io,分析受欢迎的安全信息站点、安全技术趋势、 以及提取安全工作者账号(twitter,weixin,github等)

  - 来自 @Flavor

    亮总一线渗透经验总结

    - 目录：https://github.com/Micropoor/Micro8/wiki
    - 内容： https://github.com/Micropoor/Micro8

- 2019-02-21 https://blog.trailofbits.com/201...

  How McSema Handles C++ Exceptions

- 2019-02-22
  - Turning the frustration of a mobile game into a reverse engineering training https://medium.com/@xplodwild/tu...
  - Reverse engineering of a mobile game, part 2: they updated, we dumped memory https://blog.usejournal.com/reve...
  - Reverse engineering of a mobile game, part 3: Now, it’s obfuscated https://medium.com/@xplodwild/re...

- 2019-02-23 https://christophm.github.io/int...

  Interpretable Machine Learning A Guide for Making Black Box Models Explainable.

作者花了两年时间, 经过 1219 次提交, 完成了一本 250 页的书: 可解释机器学习.

- 2019-02-24 https://github.com/ufrisk/MemPro...

  The Memory Process File System is an easy and convenient way of accessing physical memory as files a virtual file system.

  这里是作者自己对工具的介绍 http://blog.frizk.net/2019/02/re...

- 2019-02-25 https://ruoyuwang.me/bar2019/

  2019 计算机安全圈国际四大顶会之 NDSS 里关于二进制分析的论文

  - 小米手机的开源内核 https://github.com/MiCode/Xiaomi...

    本资讯来自 @dragonpower

- 2019-02-26 https://thebabush.github.io/dumb...

  Dumbo: LLVM-based Dumb Obfuscator

- 2019-02-27 https://wiki.sei.cmu.edu/conflue...

  Ensure that operations on signed integers do not result in overflow

  如何避免整型溢出的一些手段

- 2019-02-28 https://github.com/Microsoft/MSR...

  2019_02 - OffensiveCon - Growing Hypervisor 0day with Hyperseed