Technology Knowledge Base 2019-09

by bugnofree

Publish → 2019-09-01 Update → 2019-12-27

TKB 首页: https://github.com/ikey4u/tkb, 欢迎 star.

- 2019-09-01 https://www.usenix.org/system/fi...

  Automatic Wireless Protocol Reverse Engineering

- 2019-09-02 https://medium.com/@matrosov/bre...

  Breaking Through Another Side: Bypassing Firmware Security Boundaries

- 2019-09-03 https://blog.bi0s.in/2019/08/24/...

  QEMU VM Escape

- 2019-09-04 http://pwnaccelerator.github.io/...

  Hunting For Vulnerabilities in Signal

- 2019-09-05 https://docs.google.com/presenta...

  Adventures in systemd Injection

  PPT 已经备份至 datum 目录.

- 2019-09-06 https://github.com/yeggor/UEFI_R...

  UEFI 逆向工具

- 2019-09-07 https://github.com/TakahiroHaruy...

  BinDiff wrapper script for multiple binary diffing

- 2019-09-08 https://blog.trailofbits.com/201...

  Binary symbolic execution with KLEE-Native

- 2019-09-09 https://gsec.hitb.org/materials/...

  4G to 5G : New Attacks

  PDF 已经备份至 datum 目录.

- 2019-09-10 https://iwantmore.pizza/posts/dn...

  Exfiltrate Like a Pro: Using DNS over HTTPS as a C2 Channel

- 2019-09-11 https://github.com/ClaudiuGeorgi...

  A black-box obfuscation tool for Android apps

- 2019-09-12 http://scz.617.cn/misc/201909121...

  一篇很不错的文章: 闲谈Java逆向工程

- 2019-09-13 https://github.com/GuoQiang1993/...

  基于 Frida 的 Android 脱壳工具

- 2019-09-14 https://arxiv.org/pdf/1909.01752...

  反混淆的一篇论文 SATURN: Software Deobfuscation Framework Based on LLVM

- 2019-09-15 https://github.com/danigargu/deR...

  IDA Pro plugin that implements more user-friendly register and stack views

- 2019-09-16 https://thesw4rm.gitlab.io/nfque...

Command and Control via TCP Handshake

- 2019-09-17 https://github.com/chinarulezzz/...

  pixload -- Image Payload Creating tools

- 2019-09-18 https://tianma.space/post/androi...

  ROM 中的 ODEX, VDEX, APK 处理

- 2019-09-19 https://reqbin.com/

  实用工具, 好用! Post HTTP Requests Online

- 2019-09-20 https://www.sandboxie.com/Downlo...

  Windows 沙箱软件 Sandboxie.

  windows 下如果运行网上的破解软件, 直接在 Sandboxie 里运行好了, 完全不用担心电脑中毒之类的.这个软件在 9.10 号宣布免费, 之前都是要购买的.

- 2019-09-21 http://zhiheng.me/138

  C语言中数组与指针的关系, 讲的比较透彻

- 2019-09-22 https://docs.google.com/document...

  Windows Hacking/Red teaming resources

- 2019-09-23 https://blog.tetrane.com/2019/RE...

  REVEN 2.2: Python API, Automatic Recording, and more

- 2019-09-24 https://www.hex-rays.com/product...

  IDA 7.4 将支持 python3.

- 2019-09-25 https://blog.quarkslab.com/an-ex...

  An Experimental Study of Different Binary Exporters

- 2019-09-26 https://github.com/nanochess/boo...

  bootRogue, a roguelike game that fits in a boot sector (510 bytes)

- 2019-09-27 https://www.reversinghero.com

  ReversingHero : Learn Reverse Engineering (on 64bit Linux / 15 levels)

- 2019-09-28 https://medium.com/@knownsec404t...

  Java Deserialization Tool Gadgetinspector First Glimpse

- 2019-09-29 https://github.com/chrispetrou/H...

  HRShell is an HTTPS/HTTP reverse shell built with flask. It is an advanced C2 server with many features & capabilities.

- 2019-09-30 https://github.com/fireeye/flare...

  flare-emu marries IDA Pro’s binary analysis capabilities with Unicorn’s emulation framework to provide the user with an easy to use and flexible interface for scripting emulation tasks.