Technology Knowledge Base 2019-06

by bugnofree

Publish → 2019-06-01 Update → 2019-08-01

- 2019-06-01 https://github.com/invictus1306/...

  functrace - A function tracer functrace is a tool that helps to analyze a binary file with dynamic instrumentation using DynamoRIO

- 2019-06-02 https://github.com/osm0sis/AnyKe...

  AnyKernel3 - Flashable Zip Template for Kernel Releases with Ramdisk Modifications

- 2019-06-03 https://github.com/Luis-Hebendan...

  An ELF x64 binary payload injector written in c++ using the LIEF library. Injects shellcode written in fasm as relocations into the header. Execution begins at entrypoint 0 aka the header, this confuses or downright breaks debuggers. The whole first segment is rwx, this can be mitigated at runtime through an injected payload which sets the binaries segment to just rx.

- 2019-06-04

  几款网络代理工具

  chisel => https://github.com/jpillora/chisel

  goproxy => https://github.com/snail007/goproxy

- 2019-06-05 http://koyo922.github.io/2016/03...

  一篇博文(穿透公司的HTTP代理，科学上网), 几种 ssh 的利用姿势, 很强悍.

- 2019-06-06 https://github.com/lupoDharkael/...

  截图工具 flameshot, 开源, 亲试, 很不错

- 2019-06-07 https://www.youtube.com/watch?v=...

  Reverse Engineering C++ Malware With IDA Pro(youtube 视频)

- 2019-06-08 https://github.com/teemu-l/execu...

  Tool for viewing and analyzing execution traces

- 2019-06-09 https://casualhacking.io/blog/20...

  Debug UEFI code by single-stepping your Coffee Lake-S hardware CPU

- 2019-06-10 https://www.evanmiller.org/mathe...

  The Mathematical Hacker

- 2019-06-11 https://github.com/Arno0x/TCPRel...

  Tool for injecting a "TCP Relay" managed assembly into an unmanaged process

- 2019-06-12 https://github.com/n1nj4sec/pupy

  python 写的跨平台远控系统, 支持 Windows, Linux, OSX, Android.

- 2019-06-13

  视窗管理工具

  - awesomeWM https://github.com/awesomeWM/awe...
  - i3 https://i3wm.org/

- 2019-06-14 https://dog.xmu.edu.cn/2017/05/1...

  WannaCrypt蠕虫勒索病毒445端口被封的网上邻居共享方法

- 2019-06-15 https://github.com/sfyc23/Everyd...

  每日自动给女朋友发微信暖心话

- 2019-06-16 https://every-layout.dev/

  Relearn CSS layout

- 2019-06-17 https://a.ndronic.us/pre-compute...

  Pre-computed Hash Table, v. 1.0

- 2019-06-18 https://alephsecurity.com/2019/0...

  Running iOS in QEMU to an interactive bash shell (1): tutorial

- 2019-06-19 https://blog.quarkslab.com/lldba...

  LLDBagility: practical macOS kernel debugging

- 2019-06-20 https://mp.weixin.qq.com/s/SSQuR...

  除了人类,宇宙里到底还有没有其他文明?

  比较有意思的一篇文章.

- 2019-06-21 https://github.com/cool-RR/PySno...

  Python 的第三方调试库.让你通过装饰器方法,方便的知道每一行程序 运行后的结果,而不需要再手动增加 print 展示过程数据,调试程序.

- 2019-06-22 https://hackingiscool.pl/heap-ov...

  Heap overflow with stack-pivoting, format string mem leaking and first-stage ROP-ing to shellcode after making it executable on the heap - on a statically linked binary (MBE LAB7A)

- 2019-06-23 http://www.darkblue.ch/programmi...

  PE 格式

- 2019-06-24 https://www.endgame.com/blog/tec...

  十种进程注入技术, 写的很通俗易懂(看雪有翻译, 但是不太好).

  这里有一份相关的部分实现代码 https://github.com/suvllian/proc....

- 2019-06-25 https://github.com/0xffff0800/mu...

  the Leaked Muddyc3 C2 Source

- 2019-06-26 https://pan.baidu.com/s/1S76Oy2M...

  目录

```
IDAPro7.2
├── IDAPro.key
├── README.txt
├── hexrays_sdk_72.zip
├── idasdk72.7z
├── install_key.txt
├── plugins
│   ├── hexarm.dll
│   ├── hexarm64.dll
│   └── hexrays.dll
└── x64_idapronw_hexarm64w_181105_de455c480e11ef1ec91473028f4dd175.exe
```

  链接: https://pan.baidu.com/s/1S76Oy2M1EHoXATNJJZYx0Q 提取码: ksat, 解压密码 goodgoodstudy

- 2019-06-27 https://regex101.com/

  一个学习正则表达式的好网站.

下面这个简单的正则表达式是什么意思呢?

```
(^| )james=([^;]*)(;|$)
```

- 2019-06-28 https://danluu.com/branch-predic...

  How and why CPUs do “branch prediction”?

- 2019-06-29 https://www.tophertimzen.com/blo...

  Windows x64 Shellcode

- 2019-06-30 https://github.com/MiCode/Xiaomi...

  小米内核源码