Technology Knowledge Base 2019-04

by bugnofree

Publish → 2019-04-01 Update → 2019-08-01

- 2019-04-01 https://habr.com/en/post/446238/

  Exploiting signed bootloaders to circumvent UEFI Secure Boot

- 2019-04-02 https://sites.google.com/view/lt...

  Touching the Untouchables Dynamic Security Analysis of the LTE Control Plane

- 2019-04-03 https://www.dfir.training/resour...

  Windows Forensics Registry List

- 2019-04-04 推荐一波安全界的专用搜索引擎
  - https://censys.io/
  - https://www.shodan.io/
  - https://viz.greynoise.io/table
  - https://www.zoomeye.org/
  - https://wigle.net/
  - https://publicwww.com/
  - https://hunter.io/
  - https://haveibeenpwned.com/
  - https://pipl.com/
  - https://osintframework.com/
  - https://vulners.com/search?query=order:published
  - https://fofa.so/

- 2019-04-05 https://castel.dev/post/lecture-...

  How I'm able to take notes in mathematics lectures using LaTeX and Vim

- 2019-04-06 https://cstack.github.io/db_tuto...

  Let's Build a Simple Database Writing a sqlite clone from scratch in C

- 2019-04-07 https://ghidra-decompiler-docs.n...

  Ghidra - Decompiler Analysis Engine

- 2019-04-08

  A Crash Course in x86 Assembly for Reverse Engineers(pdf)

  Reverse Engineering x86 Processor Microcode(pdf)

  资料保存在 datum/ 目录.

- 2019-04-09 https://x0r19x91.github.io/2019/...

  Understanding the Movfuscator

- 2019-04-10 https://github.com/rougier/numpy...

  100 numpy exercises

- 2019-04-11 https://github.com/OUCMachineLea...

  机器&深度学习代码速查表

- 2019-04-12 https://googleprojectzero.blogsp...

  Virtually Unlimited Memory: Escaping the Chrome Sandbox

- 2019-04-13 https://www.machinelearningplus....

  Parallel Processing in Python – A Practical Guide with Examples

- 2019-04-14 https://github.com/google/tink

  Tink is a multi-language, cross-platform, open source library that provides cryptographic APIs that are secure, easy to use correctly, and hard(er) to misuse.

- 2019-04-15 https://victorzhou.com/blog/intr...

  Random Forests for Complete Beginners

- 2019-04-16 https://github.com/keepassxreboo...

  KeePassXC is a cross-platform community-driven port of the Windows application "Keepass Password Safe". https://keepassxc.org/

- 2019-04-17 https://sebastianraschka.com/Art...

  An introduction to parallel programming using Python's multiprocessing module – using Python's multiprocessing module

- 2019-04-18 https://tthtlc.wordpress.com/201...

  AFL-unicorn: What is it and how to use it?

- 2019-04-19 今天推荐几个开源的跨平台的视频剪辑软件
    - shotcut https://www.shotcut.org/download...
    - lightworks https://www.lwks.com/

  附加: https://ired.team/ Red Teaming Experiments @蒙布朗

- 2019-04-20 https://github.com/wting/autojum...

  A cd command that learns - easily navigate directories from the command line

- 2019-04-21 https://similarweb.engineering/b...

  Basic Dynamic Analysis With Frida

- 2019-04-22 https://github.com/BurntSushi/ri...

  ripgrep 快速 grep 工具.

  我最近一直在用 ag, 但是自从发现了 ripgrep, 就放弃了 ag.

  首先是用 rust 写的, 我最近狂热于 rust 语言.

  其次, 大概是唯一一个我知道的支持 unicode 范围正则搜索的工具, 比如今天 B 站视频泄漏, 有一些有意思的注释, 可以递归的只搜索中文, 方法如下

```
rg --glob "*" "[\u4e00-\u9fa5]+"
```

  然后你就能看到一些搞笑的或者让人诧异的注释.

  最后, 速度快, 比 ag, grep 都快, 支持编码, 支持 UTF-8.

  强烈推荐.

- 2019-04-23 https://syscall.eu/blog/2015/05/...

  Lesser known tricks for IDA configuration

- 2019-04-24 https://github.com/timvisee/ffse...

  Easily and securely share files from the command line. A fully featured Firefox Send client.

  依赖于火狐的一个命令行文件传输工具. 好用.

- 2019-04-25 http://moo.nac.uci.edu/~hjm/pars...

  parsyncfp - a parallel rsync wrapper for large data transfers

  据说一个很强的文件传输工具.

- 2019-04-26 https://bhamza.me/2019/04/24/Fri...

Frida Android libbinder

- 2019-04-27 https://www.secforce.com/blog/20...

  VMInjector – DLL Injection tool to unlock guest VMs

- 2019-04-28 https://github.com/tangsilian/an...

  安卓内核提权漏洞分析

- 2019-04-29 https://github.com/sixstars/star...

  official source code of *CTF2019

- 2019-04-30 https://blog.felixangell.com/vir...

  Virtual machine in C