七夜的故事

个人博客:http://qiyesafe.com

出版书籍:《Python爬虫开发与项目实战》 购买链接:https://item.jd.com/12206762.html

Python中文社区专栏作者

七夜安全博客 微信公众平台: qiye safe,及时更新技术内容

博客园 首页 新随笔 联系 管理 订阅 MILE

为什么还要记密码?

2020年4月6日

摘要: 前言 良好的习惯是人生产生复利的有力助手。 2020年 第八篇 文章,继续今年的flag:每周至少更新一篇文章。 今天的问题来源于内部的一次分享,关于密码的存储问题。 在互联网时代,大家每天接触的a pp和网站太多了,注册账户大部分的场景都需要密码。 密码的生成和存储成为了大家日常生活中常见的事情。 阅读全文

posted @ 2020-04-06 09:33 七夜的故事 阅读(609) 评论(0) 推荐(0) 编辑

2020年3月22日

linux无文件执行— fexecve 揭秘

摘要: 前言 良好的习惯是人生产生复利的有力助手。 继续2020年的flag,至少每周更一篇文章。 无文件执行 之前的文章中,我们讲到了无文件执行的方法以及混淆进程参数的方法,今天我们继续讲解一种linux上 无文件执行的技巧,是后台朋友给我的提醒,万分感谢,又学到了新的东西。 linux无文件执行,首先要提 阅读全文

والإنتان والمرامل والفراق والمرامل والفراق والمرامل والمرامل والمرامل والمرامل والمرامل والفراق والمرام

2020年3月9日

沙盒syscall监控组件: strace and wtrace

摘要: 前言 良好的习惯是人生产生复利的有力助手。 本公众号已经写了3年多了,期间时断时续,时常被事情打断,甚是烦恼。 最近在看一些时间管理方面的书,发现其实很多事情都是可以安排清楚,关键在于固 定的时间,固定的投入,形成习惯,成为良性循环。 成为习惯之后,一切就会水到渠成,2020 年慢慢来,本公众号内容还 阅读全文

posted @ 2020-03-09 10:03 七夜的故事 阅读(600) 评论(0) 推荐(0) 编辑

2019年9月15日

脚本代码混淆-Python篇-pyminifier (1)

摘要: 前言 最近研究了一下脚本语言的混淆方法,比如 python,javascript等。脚本语言属于动态语言,代码大多无法直接编译成二进制机器码,发行脚本基本上相当于暴露源码,这对于一些商业应用是无法接受 的。因此对脚本代码进行加固,成为很多应用的首选。代码加固的一项措施是代码混淆,增加逆向人员阅读代码逻。阅读全文

2019年2月10日

Python RASP 工程化:一次入侵的思考

摘要: 前言 今天讲的内容会很深,包括一些 Python的高级用法和一些自己创造的黑科技,前半部分内容你们可能听过,后半部分内容就真的是黑科技了。。。。 深入的研究和思考,总会发现很多有意思的东西。每 一次的研究,都不会是无缘无故的,下面开始我们今天的故事。(注意文末有花絮) Tips: RASP全称应用运行 阅读全文

posted @ 2019-02-10 12:57 七夜的故事 阅读(2051) 评论(0) 推荐(3) 编辑

2019年2月3日

教你学木马攻防 | 隧道木马 | 第一课

摘要: 前言 今天开始讲讲木马攻防,感觉这些内容大家应该会更感兴趣一些,就从隧道木马说起。为什么会有隧道木马这一说呢?这是根据通信协议进行分类的。讲隧道木马之前,先讲讲端口映射和转发。端口映 射和端口转发其实是一回事,原理是一样的,由于应用场景不同,才产生了不同的含义。 场景1 端口映射 端口映射的使用,以下 阅读全文

posted @ 2019-02-03 16:40 七夜的故事 阅读(1611) 评论(0) 推荐(4) 编辑

2019年1月13日

一个Python开源项目-哈勃沙箱源码剖析(下)

摘要: 前言 在上一篇中,我们讲解了哈勃沙箱的技术点,详细分析了静态检测和动态检测的流程。本篇接着对动态检测的关键技术点进行分析,包括strace,sysdig,volatility。volatility的介绍不会太深入,内存 取证这部分的研究还需要继续。 strace机制 上一篇讲到了strace和ltra 阅读全文

posted @ 2019-01-13 14:03 七夜的故事 阅读(832) 评论(0) 推荐(0) 编辑 Partie C. Land C. Company (Partie C. Company) in Edition (C. Company) in Editi

2019年1月4日

一个Python开源项目-腾讯哈勃沙箱源码剖析(上)

摘要: 前言 2019年来了,2020年还会远吗? 请把下一年的年终奖发一下,谢谢。。。 回顾逝去的2018年,最大的改变是从一名学生变成了一位工作者,不敢说自己多么的职业化,但是正在努力往那个方向走。 以前想的更多是尝试,现在需要考虑的更多是落地。学校和公司还是有很大的不一样,学到了很多东西。 2019年 阅读全文

posted @ 2019-01-04 19:40 七夜的故事 阅读(2788) 评论(0) 推荐(0) 编辑

2018年12月17日

golang高性能端口扫描

摘要: 前言 最近有个小项目的需要,使用golang写了个端口扫描工具,不得不说golang的效率确实比python快的太多了。在使用一段时间golang之后,感觉有三个方面是优于python的: 一个方面是性能优越 第 二方面是兼容性好 第三方面是可以跨平台编译成本地二进制文件,发布项目很方便。 接下来我把 阅读全文

posted @ 2018-12-17 20:33 七夜的故事 阅读(6291) 评论(4) 推荐(0) 编辑

2018年8月22日

QQ快速登录协议分析以及风险反思

摘要: 前言 众所周知,Tencent以前使用Activex的方式实施QQ快速登录,现在快速登录已经不用控件了。那现在用了什么奇葩的方法做到Web和本地的应用程序交互呢?其实猜测一下,Web和本地应用进行交互 可能采用http交互,事实也是如此。 快速登录分析 快速登陆框请求 https://xui.ptlo 阅读全文

