Eastmount
码龄9年

459
原创
2万+
粉丝
6656
获赞
4884
评论
519万+
访问

4万+
积分
13356
收藏
4
周排名
87
总排名
等级












TA的主页 私信 关注

个人博客

作者：杨秀璋
学历：本科-北京理工大学
　　硕士-北京理工大学
任教于贵州财经大学信息学院
正在武汉大学读博 砥砺前行
http://www.eastmountyxz.com

简介：自幼受贵州大山的熏陶，养成了诚实质朴的性格。经过寒窗苦读，考入BIT，为完成自己的教师梦，放弃IT、航天等工作，成为贵财一名大学教师，并想把自己所学所感真心传授给自己的学生，帮助更多陌生人。

贵州纵美路迢迢，
为负劳心此一遭。

收得破书三四本，
也堪将去教尔曹。

娜美人生，醉美生活。
他和她经历风雨，慢慢变老。

新书：
《Python网络数据爬取及分析从入门到精通（爬取篇）》《Python网络数据爬取及分析从入门到精通（分析篇）》

最新文章

[网络安全自学篇] 七十二.逆向分析之OllyDbg动态调试工具（一）基础入门及TraceMe案例分析

[网络安全自学篇] 七十.WannaCry勒索病毒复现及分析（三）蠕虫传播机制分析及IDA和OD逆向

[网络安全自学篇] 六十九.宏病毒之入门基础、防御措施、自发邮件及APT28样本分析

[网络安全自学篇] 六十八.WannaCry勒索病毒复现及分析（二）MS17-010利用及病毒解析

[网络安全自学篇] 六十七.WannaCry勒索病毒复现及分析（一）Python利用永恒之蓝及Win7勒索加密

分类专栏

Python+TensorFlow... 付费 21篇
逆向分析 1篇
知识图谱、web数据挖... 70篇
网络安全 70篇
Python爬虫之Seleniu... 34篇
编程生活 15篇

归档

2020

4月	3月	2月	1月
10篇	17篇	15篇	14篇

2019

热门文章

word2vec词向量训练及中文文本相似度计算 98299

[python] 常用正则表达式爬取网页信息及分析HTML标签总结 78926

[python爬虫] Selenium常见元素定位方法和操作的学习介绍 74233

Echarts字体和线条颜色设置操作笔记 65926

[python] 基于k-means和tfidf的文本聚类代码简单实现 63819

最新评论

[Pyhon疫情大数据分析] 四....
kun_5073：老师，代码写入文件只写入了标题那一行 应该怎么解决呢

[Pyhon疫情大数据分析] 三....
weixin_46786522：您好，运行后报错，ValueError: After pruning, no terms remain. Try a lo ...

[Python图像处理] 二十五....
Eastmount：[reply]weixin_45620656[/reply]用这张图片https://github.com/eastmountyxz， ...

[Python图像处理] 二十五....
weixin_45620656：滤镜操作失败，不知道是img还是lj_map的问题 [code=python] IndexErro ...

[Python图像处理] 二十四....
weixin_45620656：大家天南地北，再难聚，但很美。get

目录

和勒索病毒对抗

展开

¥9.90

装流程、基础语法、

订阅

友们学习，希望您们喜欢，一起进步。前
户措施等，那么如何防护呢？所以，接下
安全厂商的威胁防护措施，包括网络安全
如果存在错误或不足之处，还望告知，加

线笔记，希望您们喜欢。同时，更希望您
该系列文章对博友有所帮助，写文不易，
，一起加油喔~

经验和实践进行撰写，也推荐大家阅读参

维护，更推荐大家了解它们背后的原理，更

（二）

集

请求（二）
)
)

进程关闭）
签名复现
加持
册表及黑客常用DOS命令

BS密码

权

Asn1View等工具用法（二）

6）复现及详解

加索加密

向

御技术，既可运用于科学研究，又可用于实
智能的检测和基于词法语法的样本分析。

，这些外部威胁如何防护呢？深信服老师

黑客攻击、台积电遭到勒索病毒攻击等

流程。

毒不断扩散我们的网络。早期是以恶意代

。

来越多，该阶段衍生出很多面向应用层的
过IP端口和协议不在适用，如果不能检查

年以前就开启了监控计划，棱镜门是把它
家武器库在该时期也走进了全世界视角，
会工程的变化。

胁的对抗。APT网络攻击融合了隐蔽隧

高危漏洞、恶意软件、0day漏洞、U盘
放之后安全暴露面也不断扩大，会产生更

全人员会维护各种各样的安全设备，比如
防御。

响应能力缺失等。当前很多企业并没有这
时间。

端点，故分为网络安全问题和终端安全问

卸。

佥。

亍为。

色害。

全、协同联动。你可能会疑惑？我们企业
静态的病毒库，而且更新不具有时效性，
，威胁情报互换充分二次校验威胁。

们称为C&C互联。接着互联网主控台就

效的。

如果设备安全能力较足，越早发现越好。
防火墙查看安全日志、判断威胁等级及严重
重要。

常重要。基于大数据提供动态变化的威胁
。

的威胁校验机制判断该**IP来自哪个国家、**
该IP有害并加入黑名单，通过本地设备和

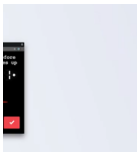
终企业面对勒索病毒、挖矿病毒、0day

云端和本地结合可视化展现风险及快速处
定位位置并给出处理建议。

处置，结合端点和网络进行双向溯源、智

RP欺骗防御及DDoS防御

防御、**人工智能算法**抵御未知病毒、不依



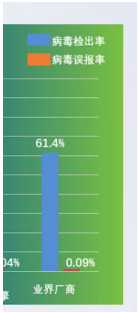
卸，从而防止企业数据泄露、网页篡改、行
判的情况，目前采用 **基于语法词法分析**

侧构建一个反方向的连接流量，由于所有
示成功了。

密服务器的文档。我们可以基于连接的频
示主机已经失陷，此时需要在网络侧定义
析及智能算法，持续监测网络异常风险。

娴隔离（主机访问控制）

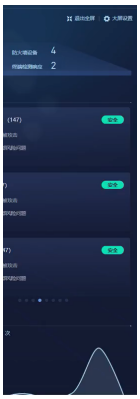
擎引擎SAVE创新**人工智能无特征技术**，能



，就认为勒索病毒上钩，把加密的进程特
本就是勒索病毒。实现单点检测和全局抑

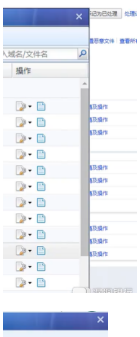
能

合



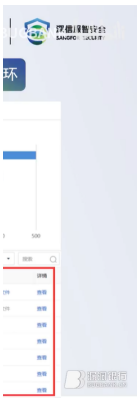
络侧会定位域名，推送给终端，终端关联

马。



，请隔离或删除文件，并加

险。



全、CNVD、瑞星等安全厂商的情报。

]学习IDA和OD逆向分析。也非常感谢老

能更透彻撰写相关文章。同时非常感谢参
得努力前行。

关注 他的留言板

收起全文

杨秀璋的专栏
希望您们 900

查看回复(1)

查看回复(2)

斤 杨秀璋的专栏
望您们喜 882

杨秀璋的专栏
讲解恶意 4627

杨秀璋的专栏
望您们喜 6612

bylfsj的博客
望您们喜 400

杨秀璋的专栏
要采用 4559

sony315的专栏
社区架 4938

帅地
是非常有必 74万+

启舰
去揭人家 38万+

薛定谔的雄猫的博客
7383

5-3

4-30

曹银飞的专栏
搜一下： 23万+

敖丙
23万+

5-1

5-1

沉默王二
烦了，想 32万+

扬帆向海的博客
10万+

5-1

4-30

Java成神之路
就业协 21万+

juwikuang的专栏
3万+

5-3

4-30

dotNet全栈开发
个人的看 17万+

趣谈前端
思想， 6739

九章算法的博客
晚会，我 17万+

敖丙
4万+

编码之外的技术博客
我又是那 9万+

HollisChuang's Blog
术细节很 8万+

敖丙
3万+

沉默王二
己的实际 14万+

沉默王二
6万+

dotNet全栈开发
有这回 5万+

Leo的博客
他就是从 5万+

龙跃十二
4万+

沉默王二
位，这令 7万+

ThinkWon的博客
nux 的体 7万+

纯洁的微笑
公司网站上 7万+

ZackSock的博客
天就给你 5万+

爪白白的个人博客
1万+

九章算法的博客
位，撕去 5万+

shenjian58的博客
但随着公司 4万+

沉默王二
可以投了无 6万+

安琪拉的博客
子书 3.回 5万+

3y
5万+

敖丙
12万+

dotNet全栈开发
不少，他们 7851

ThinkWon的博客
是什么 11万+

非著名程序员
行动，程序 2万+

shenjian58的博客
（2）男生 3万+

universsky2015的博客
？... CEO张勇 2280

ThinkWon的博客
权限的表 11万+

路人甲Java
3822

沉默王二
业。... 3万+

江南一点雨的专栏
过去，他很 3万+

不脱发的程序猿
阿里巴巴 1万+

郑晖的博客
好才是硬 2万+

启舰

这一生会容

1万+

CSDN资讯

境，那么

1万+

言 Assembly language Swift Ruby