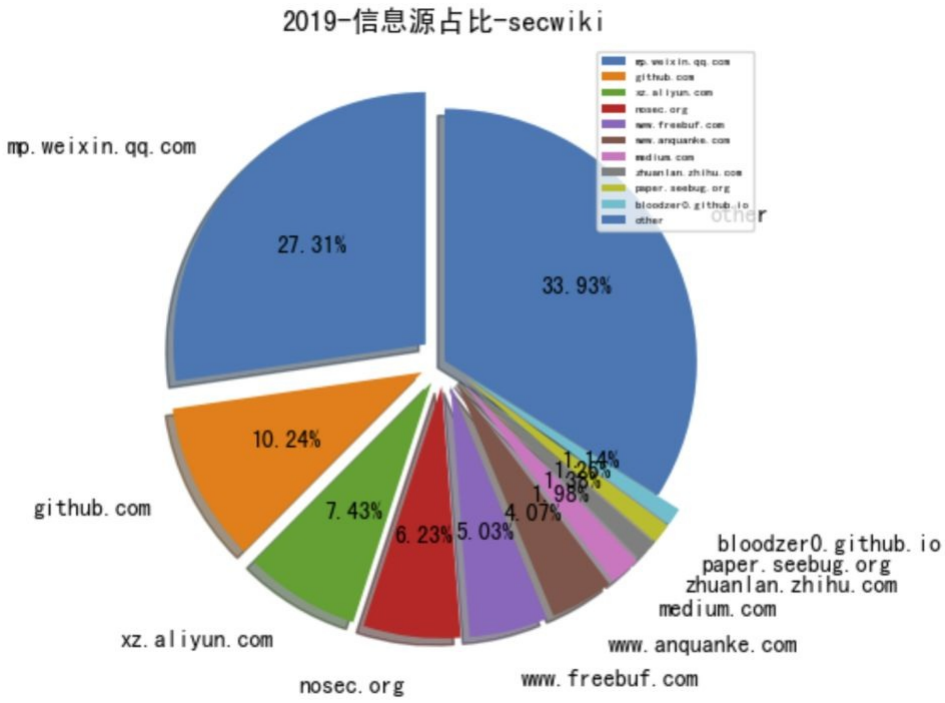
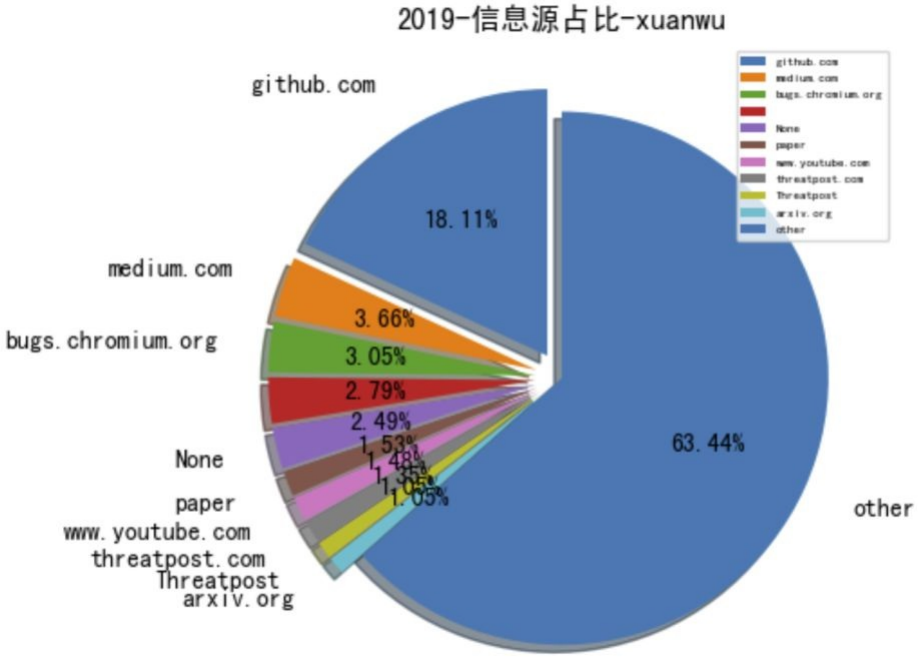
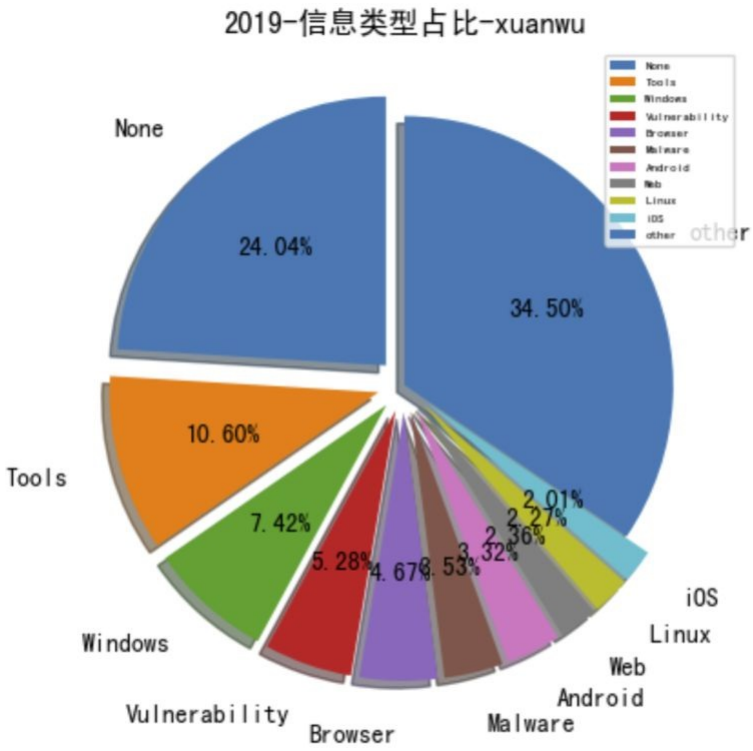
2019年度优秀安全内容合集

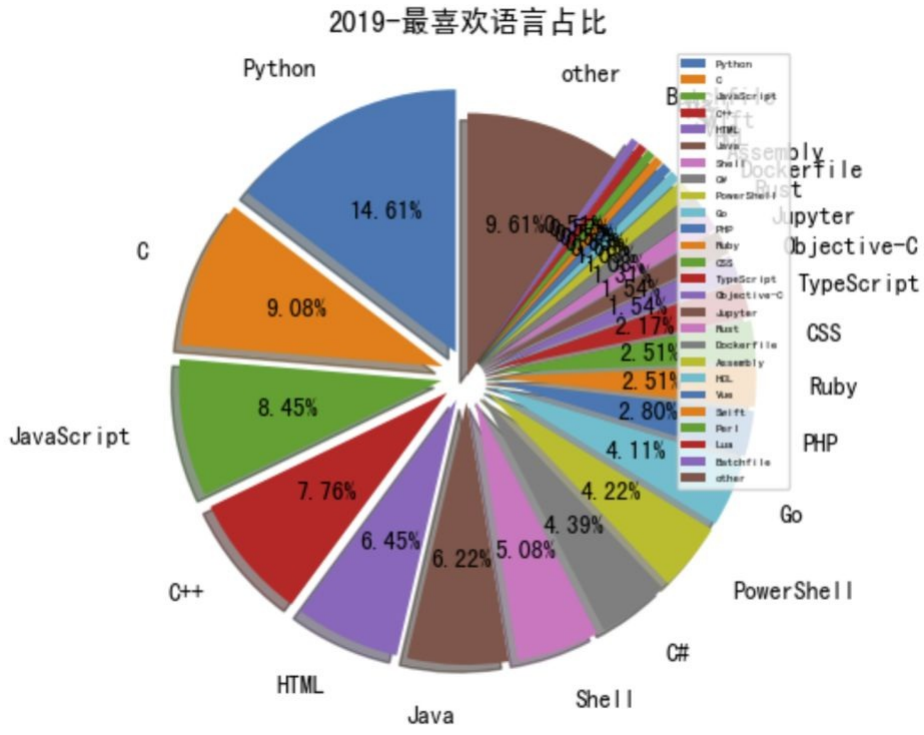
原创

2019信息源与信息类型占比









微信公众号推荐

昵称_英语	weixin_no	标题	网址
安全祖师爷		PowerShell渗透–帝国	https://mp.weixin.qq.com/s/giBR-rnpm51cDE4aude2tg
数世咨询		数世咨询：2019年网络安全大事记	https://mp.weixin.qq.com/s/APOEaYrubmWupFRPbbjfkw
飞虎行业观察	flytiger018	RSA和McAfee的2020年安全威胁预测	https://mp.weixin.qq.com/s/gUOO1kDB_wuZ32nKAZjM0g
OWASP	OWASP_中国	2019年度OWASP中国项目总结	https://mp.weixin.qq.com/s/hcdA7R36RsSV40Tnlu2fJg

昵称_英语	weixin_no	标题	网址
qz安全情报分析	外观	复制OPSEC和C2	https://mp.weixin.qq.com/s/Flz4-xk093jGN3TOECAgqQ
天地和兴	bjtdhxkj	对ICS的网络攻击20强-谈天说地Part1	https://mp.weixin.qq.com/s/H9f-z3oLDZ-fMrEax3nMaA
轩辕实验室		基于卷积神经网络的入侵检测进行检测Dos攻击	https://mp.weixin.qq.com/s/yRQwHVPuYHM67yAo15hPOw
黑客就是好玩		对乌云国防库payload的整理以及Burp辅助插件	https://mp.weixin.qq.com/s/9RHVsw-HtAfo1UuPAqXZEw
国际安全智库	郭集安权制库	“震网”十年谜底终浮水面，伊朗核计划流产源于内鬼“间谍行动”	https://mp.weixin.qq.com/s/ORW8qWCpgQFJh8-bsaIg3w
浅黑科技	千鹤池	CTF：一部黑客心灵史	https://mp.weixin.qq.com/s/wEqBaZmO8FwOyGrcWDNgYQ
腾讯安全智能	TX_Security_AI	基于图挖掘的安全事件分析	https://mp.weixin.qq.com/s/ARfMqrUxiPKmbMcV_yaluw
行业研究报告	报告88	2018-2019年网络安全行业深度报告	https://mp.weixin.qq.com/s/z-LN2AlMezEmJVekbDndcw
编程技术宇宙	ProgramUniverse	我是一个流氓软件线程	https://mp.weixin.qq.com/s/-ggUa3aWkjjHjr9VwQL9TQ
盘古实验室	盘古实验室	从研究者视角看突破研究之2010年代	https://mp.weixin.qq.com/s/UBZv0pd7Nr-o-NMxjV53RQ
牵着蜗牛遛弯儿	劳c	摘要工控CTF中网络数据分析的思路	https://mp.weixin.qq.com/s/bR1t53-YHSKWmFawT5t0Kg
维他命安全	维生素安全	卡巴斯基2019年Q3垃圾邮件与钓鱼攻击报告	https://mp.weixin.qq.com/s/JE5J6misSPhzCjyKB0MxCA
秦萧		记一次应急响应实战	https://mp.weixin.qq.com/s/ilAPsEbHnywvL1l7YXA8sQ
企业安全工作实录	小黄sec	安全运营三部曲之安全生态与安全国际	https://mp.weixin.qq.com/s/Fwk_Q7TE5pyq77_-lEp1mg
Python中文社区	python-china	微软开源可解释机器学习框架解释实践	https://mp.weixin.qq.com/s/adkQr051QFzlD4tEtPwjyQ
网信中国	卡维辛	国家互联网信息办公室关于《网络安全威胁信息发布管理办法（征求意见稿）》公开征求意见的通知	https://mp.weixin.qq.com/s/uu3fnM8OzC8JRcliJkIX8w
最高人民法院	ch_zgrmfy	司法大数据专题报告：网络犯罪特点和趋势	https://mp.weixin.qq.com/s/ZxYS6Dwa2XVOZ8ku-PbKog
404 Not F0und		从Black Hat Speaker到国内外研究者：强化学习的安全应用	https://mp.weixin.qq.com/s/YcH2P38_N4aZtGAc2ktkJw
Heysec	bloodzer007	计算机与网络安全系列书单推荐	https://mp.weixin.qq.com/s/kEH85B2L8hsTKQjaSluTVQ
复旦白泽战队	fdwhitzard	白泽带你去参会@CCS19，英国伦敦丨论文分享（上）	https://mp.weixin.qq.com/s/gYqamT3WXiyj79mjBQYRiA
安恒信息	DBAPP2013	如何基于沙箱的威胁情报平台上建造ATT&CK展示界面？	https://mp.weixin.qq.com/s/YcQRAkRRo63OnRYWokl0nw

昵称_英语	weixin_no	标题	网址
法学学术前沿	法律前沿	前沿	刘艳红：网络爬虫行为的刑事法规制
南方法治报	第1433章	广东公安“净网2019”专项行动典型网络违法犯罪案例	https://mp.weixin.qq.com/s/XlAaaZetvfLa5KO-7Q6rlg
七夜安全博客	qiye_safe	漫谈威胁建模下的安全通信	https://mp.weixin.qq.com/s/m-ouMuBGX4BhHohV52Kykg
奇门遁甲安全		突破新手入门级红蓝对抗系列之——Sysmon攻防	https://mp.weixin.qq.com/s/_RcHF1vXPp1cnzXvGWnGvQ
开放知识图谱	OpenKG-CN	论文浅尝	探索将预训练语言模型用于事件抽取和事件生成
AI科技评论	爱谈	数据挖掘领头人韩家炜教授：如何从无结构文本到有用的知识？	https://mp.weixin.qq.com/s/aKGh9wOdWsleSted_iEmBQ
星维九州		流量加密也不怕！各种姿势检测冰蝎	https://mp.weixin.qq.com/s/ciAQNdL1YJ9B1HX7TMEDzA
现代服务产业技术创新战略联盟		深度学习实体关系撤销研究概述（上）	https://mp.weixin.qq.com/s/_1bWSYleGpkJyrSfSNhVdw
腾讯技术工程	腾讯_TEG	机器学习模型可解释性的详尽介绍	https://mp.weixin.qq.com/s/JElxzuPDrbvSJjpHExaI_w
AD风险实验室		业务安全的资源层攻防时代	https://mp.weixin.qq.com/s/nkf5yRrAw-IA5_ROD6Za4g
jaxsec		Linux For Pentester：socat特权升级（中英对照）	https://mp.weixin.qq.com/s?__biz=Mzl5OTYzMjU1OA==&mid=2247483759&idx=1&sn=13cc7388d74532d0c77e2429e5c0ea2e&chksm=ec92d3aedbe55ab8573dad78ea7f0c68c3eae83c1fb585b9ee058f7d4
深度传送门	deep_deliver	RecSys 2019参会总结及推荐精读论文	https://mp.weixin.qq.com/s/NrhlEcY0-76g88-GA01kww
川云安全团队	Cyunsec	Kibana <6.6.1代码执行突破复现笔记	https://mp.weixin.qq.com/s/3r41HE3bnNHhWOw42uziTQ
穿越丛林		容器云安全防御机制动态评估与优化框架	https://mp.weixin.qq.com/s/-g2MLk7i0QBToxdE-RHjSw
App个人信息举报	app_grxxjb	专题研究	手机设备识别码类型分析
暗影安全实验室	Eversec_Lab	反间谍之旅003	https://mp.weixin.qq.com/s/ZxsyB4ELKdV84eHh6zn1iQ
电网头条	sgcctop	刚刚，国家电网公司发布《泛在电力物联网白皮书2019》	https://mp.weixin.qq.com/s/gWLm5KMfkSlhNr0ptmlYwQ
军鹰资讯	加盟信息	建立DARPA的运作机制（内附报告下载链接）	https://mp.weixin.qq.com/s/T5EqLfqSCU8JRp6Ez4vdpg
分类乐色桶		[CVE-2019-9535] lterm2命令执行的不完整重复现	https://mp.weixin.qq.com/s/4KcpS4eNGQ8bL6DTM4K0aQ
湛卢工作室	xuehao_studio	SRC突破挖掘实用技巧	https://mp.weixin.qq.com/s/g-vlNmn4uQKUnBKZ7LMJvA
90秒团队	hk90秒	域渗透总结	https://mp.weixin.qq.com/s?__biz=Mzg3NzE5OTA5NQ==&mid=2247483807&idx=1&sn=59be50aa5cc735f055db596269a857ce&chksm=cf27ea07f8506311d1c421e48d17deeebc19d569b037e0eb6to92cc3
360智库		网络战的战术实践与战略思考	https://mp.weixin.qq.com/s/NcpsTiVKaMj_NTzRydaSag
信息安全最新论文技术交流		NIST SP800-207：零信任架构草案	https://mp.weixin.qq.com/s/F0tes4QbhQyv14PFokFYuQ

昵称_英语	weixin_no	标题	网址
等级保护测评	zgdjbh	江苏网警发布第六批网络安全行政执法典型案例	https://mp.weixin.qq.com/s/zD-jjZLrAWyE4NPjpguRwg
FreeBuf企业安全	freebuf_ent	全程带阻：记一次授权网络攻防演练	https://mp.weixin.qq.com/s/BJlXOsBtPGVVU2cVs72TqQ
人民公安报	rmgabs	新中国成立70多年来公安科技信息化工作回眸	https://mp.weixin.qq.com/s/B64olNuiuu1HQUkdD3u0fg
安全乐观主义		使用方舟编译器检查Fastjson OOM问题	https://mp.weixin.qq.com/s/ornyzKd3uqjgUHEmdHGIJQ
贝塔安全实验室	BetaSecLab	网络空间搜索引擎的魅力	https://mp.weixin.qq.com/s/AdrOhuA0mpjCtdpWjPC1jg
君哥的体历	容格德利	企业如何打造有效的安全运营体系	https://mp.weixin.qq.com/s/JJkQ8S4qw0RigOoA9Xzhyw
青藤云安全资讯	青藤云	一种基于欺骗防御的入侵检测技术研究	https://mp.weixin.qq.com/s/6BEY9qpi0rfk1_T1k1IWmg
巴伦潘		基于ATT&CK的APT威胁追踪和狩猎	https://mp.weixin.qq.com/s/nqQmlWcemAGopy898l4cNg
小强说	小强电话	从ATT&CK看威胁情报的发展和应用趋势	https://mp.weixin.qq.com/s/zbAwTDZ5IuRCMkuIDo82Cw
小米安全中心	misrc_team	【技术分享】国防扫描技巧篇-Web国防扫描器	https://mp.weixin.qq.com/s/urbFms6AiUb7uu_lGj3LXQ
网信军民融合	wxjmrh	“战斗民族”俄罗斯网络空间作战研究	https://mp.weixin.qq.com/s/IHTNtsA6Pc-FGGoQoO6AUw
道法术		[法]从SOAR中超越应用安全建设强运营突围之法	https://mp.weixin.qq.com/s/sedpOhSxEGSdaxX8SACIMA
奇安信CERT		WebLogic安全研究报告	https://mp.weixin.qq.com/s/qxkV_7MZVhUYYq5QGcwCtQ
安全喷子		网络安全“圣地”之行	https://mp.weixin.qq.com/s/xxU0R5eVcP_42VVd2DQeXQ
ChaMd5安全团队	chamd5sec	De1CTF 2019-写信	https://mp.weixin.qq.com/s/EN8cch8uO8Qnfb_eewbw9w
威胁情报小屋		海莲花攻击手法概述	https://mp.weixin.qq.com/s/IrM60hbB6dWdbWxpFbO1IA
孟极实验室	梦之队	一条命令实现端口附加后门	https://mp.weixin.qq.com/s/HDZUsTbffeGhgwu1FOWQNg
码头工人	码头工人	容器日志采集利器：Filebeat深度剖析与实践	https://mp.weixin.qq.com/s/H9ExikY7bd2-YVEqGZmsOA
安全回忆录	辉辉路	Commix命令注入靶场空间过滤的绕过测试	https://mp.weixin.qq.com/s/81gI5nFHSVYR5w648Z2oJQ
安全客	安全博宝	黑帽美国2019	https://mp.weixin.qq.com/s/TCKOmHt2MbeMl6MO5zq4HQ
安比实验室	secbitlabs	初识「零知识」与「证明」	https://mp.weixin.qq.com/s/XQL_taBhPkCHGZOBc24MyQ
新兴产业研究中心		人群罢工52页深度	快速进化的十年期终端安全平台
炼石网络密码网关	密码网关	一篇读懂22种密码应用模式	https://mp.weixin.qq.com/s/07B4noqGHaQ8dHWqC_qSWQ
雷神众测	索尔斯	webshell中的分离免杀实践-java篇	https://mp.weixin.qq.com/s/RCXrCHJl4w4CTeLk_HPzQA

昵称_英语	weixin_no	标题	网址
百度安全实验室	BaiduX_lab	聪明人的笨功夫-MesaTEE安全形式化验证实践	https://mp.weixin.qq.com/s/X5PyWgQFZ11wLx8gpFtXOg
网络空间安全军民融合创新中心	m	病毒武器智能化技术现状与运用趋势	https://mp.weixin.qq.com/s/ojfjlJEdGSljrR2ptYhPSw
SDL安全实践		GitHub安全最佳实践	https://mp.weixin.qq.com/s/DRHmwihDwsoZHS8rrlwlHg
公安三所网络安全法律研究中心		《新时代的中国国防》白皮书发布，多处涉及网络安全	https://mp.weixin.qq.com/s/d85LGOF-GubW6l7bGZ2Ovw
时间之外沉浮事	s	ThreatGEN：红色vs.蓝色-在游戏中学习网络安全技能	https://mp.weixin.qq.com/s/OoCTXMYALjDQvCEOXvG2ZQ
机器学习研究会		深度学习中的Normalization模型	https://mp.weixin.qq.com/s/D1Qvh-kqcmtp6pkH-CwPmg
加特纳公司	高德纳中国	自动化在现代安全中的运用	https://mp.weixin.qq.com/s/HMvGOiUlwjMKBNE2j5qIBQ
国科军通科技	k	揭秘：中国自主可控行业全景图	https://mp.weixin.qq.com/s/7_osWtZV3UZ5KuaoIzt7rA
国科漏斗社区	Goktech_Security	线下赛AWD训练平台建造手册	https://mp.weixin.qq.com/s/VPaAYUu_W3MTOmfmgVxUjA
北极星实验室	北极星实验室	入侵WildFly	https://mp.weixin.qq.com/s/KQ_17nJBPRcOTn-rPBRKTQ
SecPulse安全脉搏	安全脉冲	网络安全学习方法论之体系的固有	https://mp.weixin.qq.com/s/yXA4BRbMfJNPQ68_-Nme6g
勾陈安全实验室	北极星实验室	刀：一个将有用的小功能加入Burp Suite快捷菜单的插件	https://mp.weixin.qq.com/s/Y03VVF3sD9N0_H6TQlxYuQ
赵武的自留地		网络安全这点屁事	https://mp.weixin.qq.com/s/kVfyoD_zRnSrQjpL4HfYAQ
遮罩	假面文章	当子域名遇上搜索引擎	https://mp.weixin.qq.com/s/yZFdVXPDh2O_qN_S1DsBPw
继之宫		威胁剑魔杂谈	https://mp.weixin.qq.com/s/wpBeoTEC7g-wFX-DA61gmA
高效运维	巨人	利用ELK建造Docker容器化应用日志中心	https://mp.weixin.qq.com/s/7A4Il1zeE5_BljzbKklnbw
安全泰式柑汁	ts_sec	2019HW行动防守总结	https://mp.weixin.qq.com/s/q2KdfZ0Wa8rkGT9i6Vjh3g
旁路	旁路 -	网络日志安全分析技巧	https://mp.weixin.qq.com/s/CtnHy9X7_csTwrG5KJvDjg
信息化协同创新专项委员会	CF-ICI	国内外颠覆性技术研究进展跟踪与研究方法总结	https://mp.weixin.qq.com/s/riKGPdyu8ekOy-WuEkyVoQ
看雪学院	益学	如何实现Https拦截进行非常规“抓包”	https://mp.weixin.qq.com/s/uPe2HHsNc44YBBUum4jogg
专注安管平台		Gartner2019年十大安全项目详解	https://mp.weixin.qq.com/s/dBw_z9oNoTRUQNVTkf1I_w
国家电网报	国家电网新闻	阿根廷全国大停电	https://mp.weixin.qq.com/s/0p_QrSpJuGSc3laQB2NMMw
新浪安全中心		自助安全扫描与代码审核系统架构实践	https://mp.weixin.qq.com/s/3N3eJzTaMwbznL_aofOjnQ
红队攻防揭秘	千秒	CobaltStrike + MetaSploit实战联动	https://mp.weixin.qq.com/s/x0txdB7tMEIg1W4v_ZK7Tg

昵称_英语	weixin_no	标题	网址
环球时报	hqsbwx	美国被爆料入侵俄罗斯电网，过渡怒怼纽约时报叛国	https://mp.weixin.qq.com/s/kfnlzwHbfNHgVXEiX2-1sg
现代军事	现代时代	解读德国情报工作建设	https://mp.weixin.qq.com/s/dW-k_LIWZt04pakFuvfX8A
网络法前哨	网络法律	公安部丨通报净网2019专项行动典型案例	https://mp.weixin.qq.com/s/P21rRO_tFo9ZDCrbDdIHGA
网安网事		网安独角兽人群罢工IPO分析（一）	https://mp.weixin.qq.com/s/YHmQDUZze_qbmebaRITKGg

组织github账号推荐

github_id	标题	网址	or
微软	AttackSurfaceAnalyzer-微软开源了一个用于分析软件对系统攻击面影响的工具，Diff软件安装前后对系统安全配置的影响	https://github.com/microsoft/AttackSurfaceAnalyzer	ht
微软	ChakraCore的3月补丁发布	https://github.com/Microsoft/ChakraCore/pull/6016	ht
贝宝	yurita：异常检测框架@ PayPal	https://github.com/paypal/yurita	ht
琴芯	英特尔（R）Boot Guard为缓解CVE-2019-11098 TOCTOU漏洞的代码实现	https://github.com/tianocore/edk2-staging/tree/BootGuardTocTouVulnerabilityMitigation	ht
愤怒	Phuzzer-用于与AFL Fuzzer交互的Python包装工具	https://github.com/angr/phuzzer	ht
mwrlabs	SharpGPOAbuse-MWR Labs开发的基于C#的工具，用于滥用GPO编辑权限攻击该GPO控制的对象	https://github.com/mwrlabs/SharpGPOA滥用	ht
pywinauto	pywinauto-Python实现的Windows平台GUI自动化测试工具，可以向UI组件发送鼠标和键盘事件	https://github.com/pywinauto/pywinauto	ht
重新提示	从UEFI固件攻击硬件可信任架构（HROT），来自进攻性2019大会	https://github.com/REhints/Publications/blob/master/Conferences/Bypassing%20Hardware%20Root%20of%20Trust/offcon2019_final.pdf	ht
现在安全	NowSecure开源的一种针对剖析iOS / macOS Apple AirDrop协议的工具，基于Frida实现	https://github.com/nowsecure/airspy	ht
nccgroup	Blackbox protobuf-NCC Group开源的用于解码和编辑Protobuf数据包的Burp Suite扩展	https://github.com/nccgroup/blackboxprotobuf	ht
CTFT培训	CTFTraining：CTF培训经典赛题复现环境	https://github.com/CTFTraining/CTFTraining	ht
模拟器	ipasim-Windows平台的一款iOS模拟器	https://github.com/ipasimulator/ipasim	没
OpenCTI平台	开放式网络威胁情报平台	https://github.com/OpenCTI-Platform/opencti	ht
Mozilla	Pwn2Own 2019中Firefox RCE突破的补丁信息（CVE-2019-9813）：https : //github.com/mozilla/gecko-dev/commit/601d226fe3690ff57287587531fd9a937298be80	https://github.com/mozilla/gecko-dev/commit/752be3958fc6f6eb83eaa4a35fae1a99dc54746e	ht
谷歌	go-containerregistry-Google开源了一个Go语言版本的Docker Registry交互工具	https://github.com/google/go-containerregistry	ht
英特尔	ModernFW-Intel开源的一个实现性项目，预先为云主机服务器提供一个最小可用的平台固件	https://github.com/intel/ModernFW	m
急速7	Metasploit框架添加了一个LibreOffice CVE-2018-16858漏洞的利用代码，该突破通过Document事件触发脚本代码执行	https://github.com/rapid7/metasploit-framework/commit/22085113ad67c0716b7b0aa6adfdaf9f7c8b48f0	ht
脸书	通过同态散列算法安全地发布更新- https://code.fb.com/security/homomorphic-hashing/	https://github.com/facebook/folly/blob/master/folly/experimental/crypto/LtHash.cpp	ht
OWASP	QRLJacking-扫描恶意二维码劫持用户登录回话的社工技术分享	https://github.com/OWASP/QRLJacking/tree/master/QRLJacker	ht
门佐	响应：Monzos实时事件响应和报告工具	https://github.com/monzo/response	ht
雷德霍克斯博士	Redhawk-软件定义无线电（SDR）的开发框架：	https://github.com/redhawksdr	ht
零平方米	ZeroMQ libzmq远程代码执行突破与利用：	https://github.com/zeromq/libzmq/issues/3351	ht
微软Edge	JsDbg：针对Microsoft Edge和基于Chromium的浏览器的调试扩展	https://github.com/MicrosoftEdge/JsDbg	没
RUB-NDS	TLS-Attacker-BurpExtension-检测TLS安全的BurpSuite插件	https://github.com/RUB-NDS/TLS-Attacker-BurpExtension	ht

github_id	标题	网址	or
夸克实验室	Quarkslab公开了很多他们团队近几年在安全会议上做过的演讲的资料	https://github.com/quarkslab/conf-presentations	ht
火眼	FireEye开源Windows事件追踪辅助工具-SilkETW	https://github.com/fireeye/SilkETW	ht
Qunarcorp	qtalk：Startalk是一款高性能的企业级im套件	https://github.com/qunarcorp/qtalk	ht
AzureAD	Microsoft身份验证库（MSAL）-AzureAD团队开源的用于Azure Active Directory认证的Python库	https://github.com/AzureAD/microsoft-authentication-library-for-python	ht
思科塔洛斯	Talos团队开源了众多用于Fuzz ClamAV杀软的种子文件	https://github.com/Cisco-Talos/clamav-fuzz-corpus	ht
平板门	文件系统Fuzz工具，相关工作已发表在Oakland19	https://github.com/sslab-gatech/janus	ht
appsecco	使用docker-kubernetes自动执行appsec和osint工作流程	https://github.com/appsecco/using-docker-kubernetes-for-automating-appsec-and-osint-workflows	ht
福克斯	adconnectdump-从Azure AD Connect服务器中补充凭证的工具	https://github.com/fox-it/adconnectdump	ht
CheckPointSW	Karta-IDA的源代码辅助快速二进制匹配插件	https://github.com/CheckPointSW/Karta	ht
站得住脚	router_badusb：路由器中的BadUSB	https://github.com/tenable/router_badusb	ht
可笑的	OPCDE 2019会议的资料公开了	https://github.com/comaeio/OPCDE/blob/master/README.md	ht
空客安全实验室	静态二进制代码分析工具BinCAT 1.1发布，支持AMD64：	https://github.com/airbus-seclab/bincat/releases/tag/v1.1	ht
HexHive	SMoTherSpectre PoC	https://github.com/HexHive/SMoTherSpectre	ht
皂素	xray：HTTP代理进行被动扫描	https://github.com/chaitin/xray	ht
o秒	tknk_scanner：基于社区的集成恶意软件识别系统	https://github.com/nao-sec/tknk_scanner	ht
超越	通过DCOM远程执行Excel 4.0 / XLM宏实现横向渗透的利用脚本	https://github.com/outflanknl/Excel4-DCOM	ht
煤火研究	DeathMetal-针对Intel AMT的攻击工具集	https://github.com/Coalfire-Research/DeathMetal	ht
googleprojectzero	WinAFL增加了基础Intel PT跟踪模式：	https://github.com/googleprojectzero/winafl/blob/master/readme_pt.md	ht
系统梦	Chashell：通过DNS进行通讯的反向Shell	https://github.com/sysdream/chashell	ht
安全突破实验室	SirepRAT：作为Windows IoT核心版上的SYSTEM的远程命令执行	https://github.com/SafeBreach-Labs/SirepRAT	ht
多恩塞奇	电负性-在基于电子实现的应用中检查安全配置不当问题的工具	https://github.com/doyensec/electronegativity	ht
RhinoSecurityLabs	Apache Axis由于代码中加载过期域名托管的资源导致的远程代码执行漏洞详情显示（CVE-2019-0227）	https://github.com/RhinoSecurityLabs/CVEs/blob/master/CVE-2019-0227/README.md	ht
数字安全	nrf5x芯片固件反编译工具	https://github.com/DigitalSecurity/nrf5x-tools	ht
每天	ML代码100天中文版	https://github.com/MLEveryday/100-Days-Of-ML-Code	ht
NLua	NLua-Lua与.NET之间的桥梁	https://github.com/NLua/NLua	ht
没什么可隐藏的	pcap_ioc：从pcap文件中提取潜在IOC的Python库	https://github.com/Nothing2Hide/pcap_ioc	ht
幽灵包	harmj0y开源了DPAPI的C＃实现工具，关于DPAPI的作用可以配合https://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/这些文章一起食用	https://github.com/GhostPack/SharpDPAPI	没
科卡米	可以生成PDF和PE的MD5冲突的脚本：	https://github.com/corkami/pocs/blob/master/collisions/README.md#pdf---pe	没
x41秒	平常在测试Java站点时常能看到500错误所引发的异常信息，该该作者提供了一个网站输入异常信息即可展示异常中所使用的Java组件的版本以及CVE编号，其做法是通过类名，方法名，代码行数做哈希之后的存入数据库，最后通过检索数据库来确定版本信息。	https://github.com/x41sec/slides/blob/master/2019-bsides-stuttgart/YourStackTracesAreLeakingCVEs.pdf	ht
爆竹	爆竹：用于无服务器计算的安全，快速的microVM	https://github.com/firecracker-microvm/firecracker	ht
米特雷攻击	BZAR-使用Bro / Zeek网络安全监控检测ATT＆CK活动的项目	https://github.com/mitre-attack/car/tree/master/implementations/bzar	m
w-数字扫描仪	w12scan：网络资产发现引擎	https://github.com/w-digital-scanner/w12scan	没
BSidesSF	BSidesSF CTF 2019源码，DockerFile及解决方案发布	https://github.com/BSidesSF/ctf-2019-release/tree/master/challenges	ht

github_id	标题	网址	or
高级威胁研究	McAfee高级威胁研究团队开源了一个辅助寻找ROP小工具的工具-xbypass，xbypass可以帮我们找到可以绕过XML文件格式字符限制的小工具地址	https://github.com/advanced-threat-research/xbypass	ht ce
w	自定义的智能卡分析测试套件，包含软件和硬件，设备使用于Chipwhisperer	https://github.com/cw-leia	没
开放系统	itops：基于Python + Django的AD \ Exchange管理系统	https://github.com/openitsystem/itops?from=时间轴	ht
大棚	同时与自定义HTML元素一起解析HTML5流。这导致流解析器对象在仍在使用时被释放。	https://github.com/sophoslabs/CVE-2018-18500/	ht
妈妈安全	陌陌开源的风控系统静态规则引擎	https://github.com/momosecurity/aswan	ht
opensec-cn	VTest-进攻测试辅助系统	https://github.com/opensec-cn/vtest	ht
redhuntlabs	很棒的资产发现资源列表	https://github.com/redhuntlabs/Awesome-Asset-Discovery	ht
QBDI	QBDI-QuarksLab开源的一种二进制动态插桩框架，支持Linux，macOS，Android，iOS和Windows。	https://github.com/QBDI/QBDI	ht
360人团队	LuWu：红队基础设施自动化部署工具	https://github.com/360-A-Team/LuWu	没
突触	CVE-2018-4193的漏洞利用	https://github.com/Synacktiv/CVE-2018-4193	ht
webarx安全	wpbullet：针对WordPress（和PHP）的静态代码分析	https://github.com/webarx-security/wpbullet	ht
蓝队实验室	利用Sysmon和MITER ATT＆CK框架实现威胁检测的实践	https://github.com/BlueTeamLabs/sentinel-attack	ht
人口普查	Windows 10 RS2 / RS3绕过GDI推锁缓解措施的两个技巧	https://github.com/CENSUS/windows_10_rs2_rs3_exploitation_primitives	ht
网飞	某些HTTP / 2实现中的几种DoS条件	https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md	ht
Riscure	用AFL Fuzz OP-TEE的系统调用	https://github.com/Riscure/optee_fuzzer	ht
秘书	用于逆向门级网表的框架工具，主要是针对FPGA逻辑门电路的逆向。	https://github.com/emsec/hal	ht
功能	用AFL-Unicorn来fuzz内核，集合了afl的覆盖率和unicorn的局部模拟执行	https://github.com/fgsect/unicorefuzz	ht be
框架	Qiling-二进制模拟执行框架，可以以沙箱模式模拟执行多种架构的代码	https://github.com/qilingframework/qiling	没
rabobank-cdc	DeTTECT-基于ATT＆CK框架，用于帮助防御团队评估日志质量，检测覆盖度的工具	https://github.com/rabobank-cdc/DeTTECT	ht
ssd-安全公开	详细介绍了iOS安全缓解措施的一步逐步化	https://github.com/ssd-secure-disclosure/typhooncon2019/blob/master/Siguza%20-%20Mitigations.pdf	ht
ucsb-seclab	sasi：基于Angr来清除二进制中重复代码的工具，相对现有工具的性能提高了主要扩展它能更加准确地完整恢复CFG	https://github.com/ucsb-seclab/sasi	ht

私人github账号推荐

github_id	标题	网址	金银丝
鲁尼夫	document-style-guide：中文技术文档的写作规范	https://github.com/ruanyf/document-style-guide	https://twitter.com/ruanyf
Justjavac	免费的计算机编程类中文书籍	https://github.com/justjavac/free-programming-books-zh_CN	https://github.com/denoland
尼克	PHP-Fuzzer-基于代码覆盖反馈信息Fuzz PHP库	https://github.com/nikic/PHP-Fuzzer	https://nikic.github.io/
邪恶的套接字	OpenSnitch-macOS Little Snitch应用防火墙的Linux移植版	https://github.com/evilsocket/opensnitch	https://www.evilsocket.net
byt3bl33d3r	利用脚本语言处理.NET有效负载，实现BYOI有效负载	https://github.com/byt3bl33d3r/Slides/blob/master/RT%20Level%209000%2B%2B_BsidesPR.pdf	https://byt3bl33d3r.github.io
s0md3v	绕过WAF的XSS检测机制研究	https://github.com/s0md3v/MyPapers/tree/master/Bypassing-XSS-detection-mechanisms	https://github.com/s0md3v
开放性	哔哩哔哩（bilibili）站的二进制疑似泄漏	https://github.com/openbilibili/go-common	没有
linux选择	适用于18个社交媒体的网络钓鱼工具	https://github.com/thelinuxchoice/shellphish	http://twitter.com/linux_choice
xdite	互联网资安风控实战	https://github.com/xdite/internet-security	http://blog.xdite.net

github_id	标题	网址	金银丝
微贫	Micro8：PHP安全新闻早8点全部文档	https://github.com/Micropoor/Micro8	没有
Skeeto	endlessh-一个伪造的SSH服务端，当攻击者连上后会不断收到SSH标语信息以耗费时间	https://github.com/skeeto/endlessh	https://nullprogram.com/
3g学生	笔试和开发技巧的集合	https://github.com/3gstudent/Pentest-and-Development-Tips	https://3gstudent.github.io/
罗伯特·戴维格拉汉姆	专家robertdavidgraham基于zerosum0x0 CVE-2019-0708扫描器的代码和开源rdesktop项目，移植了一个可以在macOS和Windows编译的CVE-2019-0708扫描器	https://github.com/robertdavidgraham/rdpscan	http://robertgraham.com
粘膜	butthax：lovense嘘buttplug利用链	https://github.com/smealum/butthax	http://smealum.net
三叉戟	reload.sh-通过SSH实现重装，恢复以及重置系统的脚本	https://github.com/trimstray/reload.sh	https://trimstray.github.io/
强制程序员	失去光泽-针对Chrome扩展程序的静态分析工具：	https://github.com/mandatoryprogrammer/tarnish	https://thehackerblog.com/
塔维索	swisstable-访问Abseil Swiss Tables的小型C封装库	https://github.com/taviso/swisstable	没有
贾姆布林	CarHackingTools：安装和配置常见的汽车黑客工具。	https://github.com/jgamblin/CarHackingTools	https://www.jerrygamblin.com
普变	一款针对Go二进制和包的取代工具	https://github.com/unixpickle/gobfuscate	https://aqnichol.com
fs0c131y	ES文件资源管理器HTTP服务端口打开漏洞披露（CVE-2019-6447）：	https://github.com/fs0c131y/ESFileExplorerOpenPortVuln	https://twitter.com/fs0c131y
里德	2018年初整理的一些内网渗透TIPS	https://github.com/Ridter/Intranet_Penetration_Tips	https://evi1cg.me
Xyntax	Xyntax公开发表了多个论文，主要方向是安全数据分析和威胁防御	https://github.com/Xyntax/slides	https://www.cdxy.me
虚拟安全	DomainFrontingLists：CDN列出的域可扩展域	https://github.com/vysecurity/DomainFrontingLists	https://github.com/vysecurity
乌林克斯	browspy：浏览器用户全部信息收集JavaScript	https://github.com/Urinx/browspy	https://urinx.github.io
醚梦	jsproxy：一个基于浏览器端JS实现的在线代理	https://github.com/EtherDream/jsproxy	没有
保罗·塞克	Shodan.io Android版官方应用程序	https://github.com/PaulSec/Shodan.io-mobile-app/issues	https://paulsec.github.io/
小伙子	w13scan：被动扫描器	https://github.com/boy-hack/w13scan?from=timeline	https://www.hacking8.com/
轻笑	OneForAll一款功能强大的子域收集工具	https://github.com/shmilylty/OneForAll	https://github.com/Qihoo360
伊斯梅尔塔斯德伦	红队硬件工具包	https://github.com/ismailtasdelen/redteam-hardware-toolkit	http://ismailtasdelen.com
Xairy	VMware虚拟机逃逸相关的资料整理	https://github.com/xairy/vmware-exploitation	https://andreyknvl.com/
潮汐	Web指纹识别技术研究与优化实现	https://github.com/TideSec/TideFinger/blob/master/Web%E6%8C%87%E7%BA%B9%E8%AF%86%E5%88%AB%E6%8A%80%E6%9C%AF%E7%A0%94%E7%A9%B6%E4%B8%8E%E4%BC%98%E5%8C%96%E5%AE%9E%E7%8E%B0.md	http://www.TideSec.com
0vercl0k	Windows 64位上的CVE-2019-9810 Firefox漏洞利用	https://github.com/0vercl0k/CVE-2019-9810	https://doar-e.github.com/
零和0x0	官方zerosum0x0公开Windows RDP RCE CVE-2019-0708突破的扫描器	https://github.com/zerosum0x0/CVE-2019-0708	https://zerosum0x0.blogspot.com
沙盒逃生者	SandboxEscaper公开了一个任务计划程序服务未正确模拟客户端令牌导致LPE的0day。	https://github.com/SandboxEscaper/polarbearrepo	没有
克隆95	Virgilio：您的数据科学在线学习新导师	https://github.com/clone95/Virgilio	没有

github_id	标题	网址	金银丝
卡特罗	一些阅读原文和Fuzzing的经验，涵盖黑盒与白盒测试	https://github.com/lcatro/Source-and-Fuzzing	https://github.com/lcatro/my-blog
jas502n	Weblogic任意文件上传突破（CVE-2019-2618）的漏洞	https://github.com/jas502n/cve-2019-2618/	没有
Vstinner	Python安全性-记录Python历史防御及补丁版本信息的Repo	https://github.com/vstinner/python-security	https://github.com/python
暴虐	Windows沙盒悖论（Flashback），来自James Forshaw	https://github.com/tyranid/infosec-presentations/blob/master/Nullcon/2019/The%20Windows%20Sandbox%20Paradox%20(Flashback).pdf	没有
Cyb3rWard0g	OSSEM-开源安全事件元数据，初步定义和共享公共信息模型以改进安全事件日志的数据标准化：	https://github.com/Cyb3rWard0g/OSSEM	https://github.com/Cyb3rWard0g
范豪瑟	AFL的社区维护版afl ++发布2.53c版本	https://github.com/vanhauser-thc/AFLplusplus/releases/tag/2.53c	https://www.mh-sec.de/
隐源性的	在PS4 6.20上的WebKit远程代码执行漏洞（CVE-2018-4441）利用	https://github.com/Cryptogenic/PS4-6.20-WebKit-Code-Execution-Exploit	https://twitter.com/SpecterDev
k8gege	K8tools：K8工具合集	https://github.com/k8gege/K8tools	http://www.cnblogs.com/k8gege
travisgoodspeed	利用GHIDRA逆向Tytera MD380的固件	https://github.com/travisgoodspeed/md380tools/wiki/GHIDRA	没有
c0ny1	xxe-lab：各种语言版本的XXE漏洞Demo	https://github.com/c0ny1/xxe-lab	http://gv7.me
池州	前两周ChiChou公开了多个macOS平台的多个应用的漏洞利用代码，包括微软Microsoft AutoUpdate，Adobe Creative Cloud Desktop以及反馈助手	https://github.com/ChiChou/sploits	https://github.com/alipay
dxa4481	结合Oauth进行XSS的高级利用以实现对目标的持久化访问：	https://github.com/dxa4481/XSSOauthPersistence	https://security.love
fdiskyou	用于枚举进程Mitigation状态的WinDbg调试器插件	https://github.com/fdiskyou/iris	http://deniable.org
丹尼尔博汉农	撤销混淆：PowerShell混淆检测框架	https://github.com/danielbohannon/Revoke-Obfuscation	http://danielbohannon.com
mame82	Logitech统一漏洞	https://github.com/mame82/UnifyingVulnsDisclosureRepo/tree/master/vulnerability_reports	https://www.twitter.com/mame82
infosecn1nja	awesome-mitre-attack-与Miter ATT＆CK攻击防御框架有关的工具和资料收集	https://github.com/infosecn1nja/awesome-mitre-attack	没有
黄酮	zodiacon开源了一个工具，用于查看内核对象类型的句柄和对象	https://github.com/zodiacon/KernelObjectView	http://scorpiosoftware.net
Ekultek	BlueKeep-Ekultek专门公开Windows RDP CVE-2019-0708 RCE PoC	https://github.com/Ekultek/BlueKeep	没有
精灵大师	dsym_obfuscate-单个加密动态符号表，并在运行时恢复的工具：	https://github.com/elfmaster/dsym_obfuscate	http://www.bitlackeys.org
0x27	思科RV320的转储配置和远程RCE的漏洞利用：	https://github.com/0x27/CiscoRV320Dump	http://0x27.me/
坦吉蒂	sec_profile：分析安全信息站点，安全趋势，安全工作者账号	https://github.com/tanjiti/sec_profile	http://tanjiti.com/
Xerub	voucher_swap-iOS 12.1.2上的P0问题1731的漏洞利用	https://github.com/xerub/voucher_swap	没有
路西法1993	cmsprint：CMS和中间件指纹库	https://github.com/Lucifer1993/cmsprint	没有
jakeajames	Patchfinder用于bazads PAC旁路中使用的偏移量	https://github.com/jakeajames/jelbrekLib/blob/master/patchfinder64.m	没有
威特	开源powershell CMD bash命令替换检测工具	https://github.com/We5ter/Flerken	https://lightrains.org
蓝灰色	Kibana CVE-2019-7609 RCE漏洞利用	https://github.com/LandGrey/CVE-2019-7609/	https://landgrey.me

github_id	标题	网址	金银丝
塞巴斯蒂安罗斯	Jint-.NET的Java解释器，在Javascript中运行.NET平台的代码	https://github.com/sebastienros/jint	http://about.me/sebastienros
鼠鼠	TikiTorch-一款允许在任意进程中执行任意ShellCode的工具	https://github.com/rasta-mouse/TikiTorch	https://github.com/ZeroPointSecurity
凯文·罗伯逊	Windows网络协议层攻击套件包括SMB LLMNR NBNS mDNS DNS	https://github.com/Kevin-Robertson/InveighZero	https://github.com/NetSPI
秘书	idenLib-识别库函数的工具集：	https://github.com/secrary/idenLib	https://secrary.com
or	CobaltStrike基于WebSocket的C2远控组件	https://github.com/xorrior/raven	https://www.xorrior.com
mjg59	mjg59为Linux内核提交了一个补丁，支持用户状态请求内核清空引用计数为0的内存页，防止重要密钥信息在进程崩溃，内存换页等场景下被泄漏。	https://github.com/mjg59/linux/commit/cd2bb1eb23ededafc2f301f8bc5561523daa96e6	https://github.com/google
404notf0und	2018-2020青年安全圈-活跃技术博主/博客	https://github.com/404notf0und/Security-Data-Analysis-and-Visualization	https://www.4o4notfound.org
Dliv3	毒液-渗透测试仪的多跳代理	https://github.com/Dliv3/Venom	https://twitter.com/D1iv3
利拜德	基于Metasploit写的一款自动化渗透测试工具	https://github.com/leebaird/discover	没有
of	JitBuddy-可以将托管的JIT本机代码反汇编的辅助功能方法：	https://github.com/xoofx/JitBuddy	https://github.com/Unity-Technologies
通兹	Internet Explorer脚本引擎远程代码执行漏洞（CVE-2018-8389）POC：	https://github.com/tunz/js-vuln-db/blob/master/jscript/CVE-2018-8389.md	http://tunz.kr
卡西史密斯	在Windows脚本主机的某些中执行任意.NET汇编代码，来自DerbyCon2019	https://github.com/caseysmithrc/DerbyCon2019	没有
Grayddq	GScan：Linux主机侧清单的自动综合化检测	https://github.com/grayddq/GScan	没有
汉诺布	Apache不准备修复的UAF突破公开：	https://github.com/hannob/apache-uaf/	https://hboeck.de/
Tuhinshubhra	ExtAnalysis：浏览器扩展分析框架	https://github.com/Tuhinshubhra/ExtAnalysis	https://twitter.com/r3dhax0r
0x4D31	大规模网络指纹探测与数据聚类分析，作者利用网络指纹信息追踪攻击者及攻击工具，同时发布了一个工具FATT。来自AusCERT 2019会议	https://github.com/0x4D31/演示	https://github.com/salesforce
猪笼草	Python工匠	https://github.com/piglei/one-python-craftsman	http://www.zlovezl.cn
rvrsh3ll	将shellcode隐藏在资源文件中再通过CPL加载执行的POC	https://github.com/rvrsh3ll/CPLResourceRunner	没有
ExpLife0011	优秀Windows内核防御利用方向资源收集	https://github.com/ExpLife0011/awesome-windows-kernel-security-development/blob/master/README.md	没有
德尔克詹姆	Kerberos无约束委派滥用工具包	https://github.com/dirkjanm/krbrelayx	没有
幻影0301	PTEye：代理黑盒突破审计工具	https://github.com/phantom0301/PTEye	http://phantom0301.github.io/
意大利面食	丰田公司开发了一套汽车ECU系统的测试工具，包含软件和硬件，repo里面有这套工具的相关介绍，目前应该是在售的状态。	https://github.com/pasta-auto/PASTA1.0	没有
7kb风暴	7kbscan-WebPathBrute Web路径暴力探测工具	https://github.com/7kbstorm/7kbscan-WebPathBrute	https://www.7kb.org
赌注	2019腾讯广告算法大赛完整代码（冠军）	https://github.com/bettenW/Tencent2019_Finals_Rank1st	http://zhuanlan.zhihu.com/DataAl
怀阿图	秘鲁语：网络资产防御扫描器/扫描框架	https://github.com/WyAtu/Perun	没有

github_id	标题	网址	金银丝
rk700	之前推过AFL-Unicorn项目可以让AFL fuzz能用Unicorn模拟的闭源binary，这个uniFuzzer项目很类似，是要把libfuzzer应用在闭源binary上	https://github.com/rk700/uniFuzzer//	http://rk700.github.io
梅塔尔	令人敬畏的网络安全蓝队-蓝队防御相关的工具，文章资料收集	https://github.com/meitar/awesome-cybersecurity-blueteam	https://web.archive.org/web/20190206200 i-am-publicly-disassociating-myself-from-th
斯塔德拉	Git Fetch相关的突破利用研究（CVE-2018-11235& CVE-2018-16873）	https://github.com/staaldraad/troopers19/	https://github.com/heroku
芯子	SharpSploit-C＃语言编写的基于.NET的后渗透测试工具	https://github.com/cobbr/SharpSploit	https://cobbr.io
gh0stkey	PoCBox-进攻测试验证辅助平台	https://github.com/gh0stkey/PoCBox	https://gh0st.cn
RUB-SysSec	NEMO：一种猜测密码的工具，通过使用马尔可夫模型可以更高效地选择变异策略	https://github.com/RUB-SysSec/NEMO//	https://syssec.rub.de
米奇	Stracciatella-绕过AMSI和脚本块日志记录加载执行PowerShell脚本的工具	https://github.com/mgeeky/Stracciatella	https://www.linkedin.com/in/mariuszban/
叶伊敏特素	浏览器，缓解措施，内核等漏洞利用相关研究	https://github.com/yeyintminthuhtut/Awesome-Advanced-Windows-Exploitation-References	http://pentest.space
1991年	2019年针对API安全的4点建议	https://github.com/neal1991/articles-translator/blob/master/2019%E5%B9%B4%E9%92%88%E5%AF%B9API%E5%AE%89%E5%85%A8%E7%9A%844%E7%82%B9%E5%BB%BA%E8%AE%AE.md	https://madneal.com
病毒狂	I-See-You：Bash和Javascript工具查找用户的确切位置	https://github.com/Viralmaniar/I-See-You	https://twitter.com/maniarviral
bcoles	bcoles收集的Linux内核Exploits	https://github.com/bcoles/kernel-exploits	https://itsecuritysolutions.org
hlldz	APC-PPID-通过APC注入创建进程并伪造父进程的项目	https://github.com/hlldz/APC-PPID	https://artofpwn.com
zer0yu	网络空间安全的RSS订阅	https://github.com/zer0yu/CyberSecurityRSS	http://zeroyu.xyz/
Pyn3rd	Apache Tomcat远程代码执行漏洞（CVE-2019-0232），可以通过Windows enableCmdLineArguments触发	https://github.com/pyn3rd/CVE-2019-0232/	https://twitter.com/pyn3rd

medium_xuanwu推荐

标题	网址
从Xceedium Xsuite远程代码执行扩展到域管权限的实际案例	http://medium.com/@DanielC7/remote-code-execution-gaining-domain-admin-privileges-due-to-a-typo-dbf8773df767
MikroTik RouterOS SMB服务无需认证的RCE漏洞挖掘与利用（CVE-2018–7445）	http://medium.com/@maxi./finding-and-exploiting-cve-2018-7445-f3103f163cc1
通过Excel文件执行命令以反弹Meterpreter shell的不同方法	http://medium.com/@Bank_Security/ms-excel-weaponization-techniques-79ac51610bf5
微软针对云网络安全打造的SIEM解决方案-Azure Sentinel介绍	http://medium.com/@maarten.goet/microsoft-azure-sentinel-not-your-daddys-splunk-3775bda28f39
红队评估物理环境安全性常用的五种方式	http://medium.com/@adam.toscher/top-5-ways-the-red-team-breached-and-assessed-the-physical-environment-fa567695b354
Vimeo从SSRF到SSH密钥泄漏	http://medium.com/@rootxharsh_90844/vimeo-ssrf-with-code-execution-potential-68c774ba7c1e
编写受密码保护的反弹Shell（Linux / x64）	http://medium.com/@0x0FFB347/writing-a-password-protected-reverse-shell-linux-x64-5f4d3a28d91a
我是如何在redacted.com挖到Blind XSS的	http://medium.com/@newp_th/how-i-find-blind-xss-vulnerability-in-redacted-com-33af18b56869
如何为WinDbg和LLDB编写ClrMD扩展	http://medium.com/@kevingosse/writing-clrmd-extensions-for-windbg-and-lldb-916427956f66
从RCE到LDAP信息泄漏	http://medium.com/@thbcn/from-rce-to-ldap-access-9ce4f9d2fd78
分析Metasploit Linux / x64反向Shell负载	http://medium.com/@0x0FFB347/analysis-of-some-metasploit-network-payloads-linux-x64-ab8a8d11bbae
PostgreSQL从9.3到11.2版本的认证用户任意命令执行突破披露（CVE-2019–9193）	http://medium.com/greenwolf-security/authenticated-arbitrary-command-execution-on-postgresql-9-3-latest-cd18945914d5
跨站点内容和状态类型泄漏	http://medium.com/@terjanq/cross-site-content-and-status-types-leakage-ef2dab0a492

标题	网址
XPWN 2018 Safari沙箱逃脱中文版：https ://weibo.com/ttarticle/p/show?id=2309404354112320866984	http://medium.com/p/one-liner-safari-sandbox-escape-exploit-91082ddbe6ef
使用Sboxr自动化发现和利用DOM XSS-第1部分	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.appsecco.com%2Fautomating-discovery-and-exploiting-dom-client-xss-vulnerabilities-using-sboxr-part- 1-2e55c120c9e1
使用BadUSB攻击路由设备控制目标网络	http://medium.com/tenable-techblog/owning-the-network-with-badusb-72daa45d1b00
使用Sboxr自动发现并利用DOM XSS漏洞-第2部分	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.appsecco.com%2Fautomating-discovery-and-exploiting-dom-client-xss-vulnerabilities-using-sboxr-part- 2-3b5c494148e0
使用ATT＆CK Datamap可视化展示潜在威胁	http://medium.com/@olafhartong/assess-your-data-potential-with-att-ck-datamap-f44884cfed11
滥用macOS的Folder Actions功能实现持久化控制	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fposts.specterops.io%2Ffolder-actions-for-persistence-on-macos-8923f222343d
深入了解Apple的二进制属性列表plist格式	http://medium.com/@karaiskc/understanding-apples-binary-property-list-format-281e6da00dbd
使用SSH隧道进行端口转发和建造Socks5代理	http://medium.com/tarkalabs/power-of-ssh-tunneling-cf82bc56da67
绕过域账户认证失败锁定次数限制的技巧	http://medium.com/@markmotig/bypassing-ad-account-lockout-for-a-compromised-account-5c908d663de8
利用HTML注入入侵泄漏用户数据	http://medium.com/@d0nut/better-exfusion-via-html-injection-31c72a2dae8b
作者发现阿里巴巴多个站点加载了alipay某个域名，该域名中返回的内容是可以通过cookie控制的，于是作者在alipay其他的子域名上找到了一处反射型XSS（曲折的绕过了WAF，cookie设置的限制），通过此XSS设置上恶意的cookie后来完成账号的窃取。	http://link.medium.com/jNotfTcVSV
Rootpipe Reborn-macOS TimeMachine诊断扩展Root命令注入细分分析	http://medium.com/@CodeColorist/rootpipe-reborn-part-i-cve-2019-8513-timemachine-root-command-injection-47e056b3cb43?source=friends_link&sk=3970823f97714fac1d04d75325e3cbac
基于P4wnP1实现将Raspberry Pi Zero W变成坏的USB设备，最终实现逃脱杀毒软件检测的安全研究	http://medium.com/@fbotes2/advance-av-evasion-symantec-and-p4wnp1-usb-c7899bcbc6af
Elliot Alderson通过分析发了一个邮箱验证的漏洞，成功以Tchap员工的身份登录了软件。	http://medium.com/@fs0c131y/tchap-the-super-not-secure-app-of-the-french-government-84b31517d144?source=friends_link&sk=59e15e44ba75dd78d7248262a4c8f0b7
我是如何在OWASP ModSecurity核心规则集（CRS）中发现5个正则表达式拒绝服务漏洞的	http://medium.com/@somdevsangwan/how-i-found-5-redos-vulnerabilities-in-mod-security-crs-ce8474877e6e?sk=c648522452l5d6fead387acbd394b7db
Venator-SpectreOps开发的一种用于macOS平台的恶意软件行为检测的工具，这个工具会搜集可能会暴露恶意软件行为痕迹的信息，包括：launch_agents，浏览器扩展，bash_history等等	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fposts.specterops.io%2Fintroducing-venator-a-macos-tool-for-proactive-detection-34055a017e56%3Fsource%3Drss- --- f05f8696e3cc --- 4
如何利用Confluence未授权RCE突破（CVE-2019-3396）在6小时内黑掉50+公司	http://link.medium.com/l0lpOUJXeW
组合4个CSRF进攻搞定公司的账户	http://medium.com/a-bugz-life/4x-csrfs-chained-for-company-account-takeover-f9fada416986
CORS（跨域资源共享）错误配置突破的高级利用	http://link.medium.com/UTKkk4wvGW
利用Slack Windows版本客户端的入侵窃取Slack用户下载的所有文件	http://link.medium.com/eFLkuCEvLW
WordPress 5.0.0 RCE（CVE-2019–6977）漏洞的详细分析	http://medium.com/@knownsec404team/the-detailed-analysis-of-wordpress-5-0-rce-a171ed719681
CVE-2019–0708 Windows RDP RCE漏洞的影响面有多大，以及如何利用Sigma规则，弹性，ArcSight检测这种攻击	http://medium.com/@ab_65156/proactive-detection-content-cve-2019-0708-vs-mitre-att-ck-sigma-elastic-and-arcsight-22f9ebae7d82
建造一个Drupal Core RCE（CVE-2019–6340）突破的蜜罐	http://medium.com/@SecurityBender/building-a-real-world-web-honeypot-for-cve-2019-6340-rce-in-drupal-core-f4240f989c3f
本地攻击三星手机ContainerAgent APP的导出组件，导致持久化的本地DOS	http://medium.com/@fs0c131y/how-to-brick-all-samsung-phones-6aae4389bea
基于Windows渗透构造的CTF，包括完整的域渗透流程，还是值得一看。	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.ettic.ca%2Fnorthsec-2019-windows-track-writeup-69d5bcf06abd
V8引擎编译及调试环境的建造	http://medium.com/@stankoja/v8-bug-hunting-part-1-setting-up-the-debug-environment-7ef34dc6f2de
作者详细介绍了逆向分析Spotify.app并挂接其功能获取数据的过程。	http://medium.com/@lerner98/skiptracing-reversing-spotify-app-3a6df367287d
V8 Bug Hunting之JS类型对象的内存布局	http://medium.com/@stankoja/v8-bug-hunting-part-2-memory-representation-of-js-types-ea37571276b8
ATT＆CK威胁建模方法在企业威胁感知方面的应用，分3个不同的等级针对不同规模的企业	http://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f
Windows SetThreadContext API剖析	http://medium.com/tenable-techblog/api-series-setthreadcontext-d08c9f84458d
在云上建造一个Burp Collaborator服务器的方法	http://medium.com/bugbountywriteup/deploy-a-private-burp-collaborator-server-in-azure-f0d932ae1d70
Mybb 18.20存储类型XSS突破以及RCE利用过程分析	http://medium.com/@knownsec404team/the-analysis-of-mybb-18-20-from-stored-xss-to-rce-7234d7cc0e72?postPublishedType=initial
文章详细介绍了从越狱手机中转储app的二进制文件，获取类及方法的方法，利用frida hook程序，最后注入了一个动态库到目标程序的过程。	http://medium.com/@lerner98/skiptracing-part-2-ios-3c610205858b
利用“白”的程序执行“黑”的程序来绕过杀毒检测	http://medium.com/@reegun/update-nuget-squirrel-uncontrol-endpoints-leads-to-arbitrary-code-execution-b55295144b56
对Arlo相机设备功能及安全性的一次深入分析	http://medium.com/tenable-techblog/an-analysis-of-arlo-6f1b691236b5
在这个系列中，作者非常详细列出了各类工具的使用方法，需要输入的命令和一些问题的解决方法，可以说很良心了，是调试三星手机内核很好的入门篇	http://medium.com/@alex91ar/debugging-the-samsung-android-kernel-part-3-c27e916c9a7d
Windows系统雷蛇环绕音频服务1.1.63.0版本存在文件/目录权限设置不当导致本地局部权衡	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fposts.specterops.io%2Fcve-2019-13142-razer-surround-1-1-63-0-eop-f18c52b8be0c
视频会议系统Zoom的Mac客户端存在多个安全漏洞，可能导致拒绝服务和信息泄漏	http://medium.com/@jonathan.leitschuh/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

标题	网址
Citrix SD-WAN下三个突破及攻击手段介绍	http://medium.com/tenable-techblog/an-exploit-chain-against-citrix-sd-wan-709db08fb4ac
Jira把联系管理员处的表单数据当成freemarker模板解析，导致前台RCE。	http://medium.com/@ruvlol/rce-in-jira-cve-2019-11581-901b845f0f
Comodo杀毒软件存在安全漏洞，可以从其沙箱中直接获得SYSTEM权限	http://medium.com/tenable-techblog/comodo-from-sandbox-to-system-cve-2019-3969-b6a34cc85e67
AI与机器学习的安全性问题研究	http://link.medium.com/5FVO5CWpAY
Opera Android浏览器地址栏欺骗（CVE-2019–12278）漏洞的分析	http://medium.com/@justm0rph3u5/opera-android-address-bar-spoofing-cve-2019-12278-9ffcfd6c508c
上周发生的Capital One数据泄漏事件的技术分析	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.cloudsploit.com%2Fa-technical-analysis-of-the-capital-one-hack-a9b43d7c8aea%3F
来自DEF CON 27会议上针对MikroTik RouterOS系统的漏洞利用研究	http://medium.com/tenable-techblog/routeros-post-exploitation-784c08044790
基于时间的横向信道攻击，实现准确识别请求是被WAF直接拦截或被WAF过滤后传递到服务器。	http://medium.com/@0xInfection/fingerprinting-waf-rules-via-timing-based-side-channel-attacks-cd29c48fb56
逃逸基于机器学习技术的恶意软件检测，这是作者今年参加DEFCON AI Village的Writeup	http://medium.com/@william.fleshman/evading-machine-learning-malware-classifiers-ce52dabdb713
从Windows客户端防御利用到获取Kubernetes Cluster管理员权限	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.appsecco.com%2Ffrom-thick-client-exploitation-to-becoming-kubernetes-cluster-admin-the-story-一个有趣的错误我们fe92a7e70aa2
Dell XPS上的Qualcomm驱动程序	http://medium.com/tenable-techblog/kernel-write-what-where-in-qualcomm-driver-lpe-f08389f6fce9
重新想象杀人逃脱行为的检测	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fposts.specterops.io%2Fyou-can-run-but-you-cant-hide-detecting-process-reimaging-behavior- e6bb9a10c40b
作者介绍了自己的工具Shhmon卸载Sysmon的相关技术分析	http://medium.com/p/shhmon-silencing-sysmon-via-driver-unload-682b5be57650
利用FireEye开源的SilkETW工具实现基于ETW Events的威胁检测	http://medium.com/threat-hunters-forge/threat-hunting-with-etw-events-and-helk-part-1-installing-silketw-6eb74815e4a0
利用上传文件到服务器和服务器上传文件到Amazon S3的时间空隙，通过本地文件包含实现了RCE。	http://medium.com/@YoKoKho/race-condition-that-could-result-to-rce-a-story-with-an-app-that-temporary-stored-an-uploaded-9a4065368ba3
一个DLL注入导致的本地提权扩展	http://medium.com/@bazyli.michal/more-than-a-penetration-test-cve-2019-1082-647ba2e59034
Microsoft Windows Windows威胁智能机制向线程注入APC的方法-采用kenel APC向线程注入用户APC	http://medium.com/@philiptsukerman/bypassing-the-microsoft-windows-threat-intelligence-kernel-apc-injection-sensor-92266433e0b0
对基于物联网的出勤设备进行渗透测试	http://medium.com/bugbountywriteup/pentesting-an-iot-based-biometric-attendance-device-10c0efd69392
XSS高级技巧之Bypass大写过滤器	http://medium.com/@Master_SEC/bypass-uppercase-filters-like-a-pro-xss-advanced-methods-daf7a82673ce
入门教程-如何探索网络摄像头的突破（固件）	http://medium.com/@knownsec404team/getting-started-tutorial-how-to-explore-the-camera-vulnerability-firmware-c405e25ed177
如何使用使用burp套件扩展插件（taborator）利用exploit远程文件包含/带外资源加载（HTTP）测试	http://link.medium.com/RKQJyWPJSZ
Proftpd被发现裂缝溢出裂缝（CVE-2019–18217），影响1.3.6b之前的版本	http://medium.com/@social_62682/proftpd-buffer-overflow-cve-2019-18217-281503c527e6
在线WebAssembly终端-某个在浏览器中直接执行	http://medium.com/wasmer/webassembly-sh-408b010c14db
了解usbmux和iOS锁定服务，了解iTunes，Xcode是如何与iOS设备交互的	http://medium.com/@jon.gabilondo.angulo_7635/understanding-usbmux-and-the-ios-lockdown-service-7f2a1dfd07ae
Facebook Creator Studio Session过期绕过突破的分析	http://medium.com/bugbountywriteup/session-expiration-bypass-in-facebook-creator-app-b4f65cc64ce4?source=rss----7b722bfd1b8d---4
作者分析入侵JSON Web令牌（JWT）过程	http://link.medium.com/2rXn12vA80
wolfssl CVE-2019–18840被发现堆重叠裂缝	http://medium.com/@social_62682/heap-overflow-in-wolfssl-cve-2019-18840-185d233c27de
Symantec终端防护软件本地系统提权突破（CVE-2019–12757）的分析	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fposts.specterops.io%2Fcve-2019-12757-local-privilege-escalation-in-symantec-endpoint-protection-1f7fd5c859c6
在Node.JS中实现Steam API介绍	http://medium.com/florence-development/working-with-node-js-stream-api-60c12437a1be
利用红外线攻击Android Smart TV的细节	http://medium.com/@drakkars/hacking-an-android-tv-in-2-minutes-7b6f29518ff3
调试三星Android内核第三部分：如何为三星内核启用USB串行调试	http://medium.com/@alex91ar/debugging-the-samsung-android-kernel-part-3-a6a7f762fcd6?source=friends_link&sk=635b789114be318db3b28e454b4069d7
入侵XML数据-使用XPATH注入获得数据访问	http://link.medium.com/WJD9QOxs91
从LTE服务退回到3G-CSFB详解	http://link.medium.com/3HOw2oexi2
利用DeviceIoControl清理NTFS的元数据	http://medium.com/@grzegorztworek/cleaning-ntfs-artifacts-with-fsctl-clean-volume-metadata-bd29afef290c?source=friends_link&sk=6ef94fc3bdf764386990c6644905fcbb
一款新的恶意广告样本macOS Bundlore加载程序分析	http://medium.com/m/global-identity?redirectUrl=https%3A%2F%2Fblog.confiant.com%2Fnew-macos-bundlore-loader-analysis-ca16d19c058c
作者介绍在Chrome中使用WebRTC ICE服务器进行对端口扫描的新技术。	http://medium.com/tenable-techblog/using-webrtc-ice-servers-for-port-scanning-in-chrome-ce17b19dd474
威胁报告ATT＆CK映射器（TRAM）是基于Web的工具，可自动提取对手的行为进行分析，将其映射到ATT＆CK。	http://medium.com/mitre-attack/automating-mapping-to-attack-tram-1bb1b44bda76
滥用SourceMappingURL实现Javascript反调试	http://medium.com/@weizmangal/javascript-anti-debugging-some-next-level-sh-t-part-1-abusing-sourcemappingurl-da91ff948e66
作者分析Apache Olingo中存在反序列化安全漏洞（CVE-2019-17556）	http://medium.com/bugbountywriteup/cve-2019-17556-unsafe-deserialization-in-apache-olingo-8ebb41b66817?source=rss----7b722bfd1b8d---4

标题	网址
CVE-2019-17556：Apache Olingo中的不安全反序列化	http://medium.com/bugbountywriteup/cve-2019-17556-unsafe-deserialization-in-apache-olingo-8ebb41b66817
双因素认证（2FA）绕过技术的总结	http://medium.com/@surendirans7777/2fa-bypass-techniques-32ec135fb7fe

medium_secwiki推荐

标题	网址
SVG XLink SSRF指纹库版本– Arbaz H ...	https://medium.com/@arbazhussain/svg-xlink-ssrf-fingerprinting-libraries-version-450ebecc2f3c
发现和利用CVE-2018–7445	https://medium.com/@maxi./finding-and-exploiting-cve-2018-7445-f3103f163cc1
IBM Websphere中的主机头中毒	https://medium.com/@x41x41x41/host-header-poisoning-in-ibm-websphere-3d459a990f00
适用于iOS的ProtonMail中的3个XSS – Vladimir Metnew –中	https://medium.com/@vladimirmetnew/3-xss-in-protonmail-for-ios-95f8e4b17054
编写密码保护的反向Shell（Linux / x64）	https://medium.com/@0x0FFB347/writing-a-password-protected-reverse-shell-linux-x64-5f4d3a28d91a
编写自定义Shellcode编码器	https://medium.com/@0x0FFB347/writing-a-custom-shellcode-encoder-31816e767611
SigintOS：无线渗透测试发行版	https://medium.com/@tomac/sigintos-a-wireless-pentest-distro-review-a7ea93ee8f8b
SolarWinds数据库性能分析器中反映的XSS	https://medium.com/greenwolf-security/reflected-xss-in-solarwinds-database-performance-analyzer-988bd7a5cd5
使用BadUSB攻击路由设备控制目标网络	https://medium.com/tenable-techblog/owning-the-network-with-badusb-72daa45d1b00
Android斗篷和匕首攻击	https://medium.com/@targetpractice/cloak-and-dagger-malware-techniques-demystified-c4d8a035b94e
多个漏洞+ WAF绕过帐户接管	https://medium.com/@y.shahinzadeh/chaining-multiple-vulnerabilities-waf-bypass-to-account-takeover-in-almost-all-alibabas-websites-f8643eaa2855
如何开始学习数字取证	https://medium.com/@a.alwashli/how-to-start-learning-digital-forensics-8038bcc9af6a
一个旧的Cisco OpenSSH Bug	https://medium.com/tenable-techblog/an-old-cisco-openssh-bug-342ce6679f61
从Slack用户窃取下载	https://medium.com/tenable-techblog/stealing-downloads-from-slack-users-be6829a55f63
反向Golang二进制文件：第2部分	https://medium.com/@nishanmaharjan17/reversing-golang-binaries-part-2-26f522264d01
反向Golang二进制文件：第1部分	https://medium.com/@nishanmaharjan17/reversing-golang-binaries-part-1-c273b2ca5333
更秘密的电报	https://medium.com/@labunskya/secret-telegrams-bdd2035b6e84
SIM卡端口黑客的详细信息	https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124?sk=4c29b27bacb2eff038ec8fe4d40cd615
在无监督学习中检测模式	https://medium.com/code-gin/detecting-patterns-with-unsupervised-learning-88ba737d4f34
CVE-2019–0708的调试入门	https://medium.com/@straightblast426/a-debugging-primer-with-cve-2019-0708-ccfa266682f6
ATT＆CK入门：威胁情报	https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f
ATT＆CK入门：检测和分析	https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0
使用ATT＆CK数据图评估您的数据潜力	https://medium.com/@olafhartong/assess-your-data-potential-with-att-ck-datamap-f44884cfed11
如果您是网络入门的十大阅读清单...	https://medium.com/katies-five-cents/a-top-10-reading-list-if-youre-getting-started-in-cyber-threat-intelligence-c11a18fc9798
CTI阅读清单	https://medium.com/@sroberts/cti-reading-list-a93ccdd7469c
假设假设扩展的辅助损失优化	https://medium.com/@jason_trost/auxiliary-loss-optimization-for-hypothesis-augmentation-for-dga-domain-detection-98c382082514
使用FwAnalyzer自动化固件安全	https://medium.com/cruise/firmware-security-fwanalyzer-dcbd95cef717
流星盲NoSQL注入	https://medium.com/rangeforce/meteor-blind-nosql-injection-29211775cd01
RouterOS开发后	https://medium.com/tenable-techblog/routeros-post-exploitation-784c08044790
面向黑客和OSINT研究人员的十大浏览器扩展	https://medium.com/@NullByteWht/top-10-browser-extensions-for-hackers-osint-researchers-fca19b469158
恶意文件针对越南官员	https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a
威胁猎人剧本+主数据集+ BinderHub =基础设施...	https://medium.com/threat-hunters-forge/threat-hunter-playbook-mordor-datasets-binderhub-open-infrastructure-for-open-8c8aee3d8b4
InfoSec的千篇一律	https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1

来源：https://github.com/tanjiti