



ISC 互联网安全大会



360 互联网安全中心

国内黑客论坛在网络犯罪中的作用及应对策略

陈石 北京市公安局网络安全保卫总队

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

(原“中国互联网安全大会”)

目录

- 一、国内黑客论坛在网络犯罪中的作用
- 二、国内黑客论坛的分类及应对策略
- 三、我局侦办非法“黑客论坛案件”案例介绍
- 四、经验交流

一、国内黑客论坛在网络犯罪中的作用

黑客群体学习模式主要在于黑客把学到的技术和工具分享给他人，通过网络传递自己的技术成果。互联网的快速发展和高度的开放性让黑客群体拥有了更高的合作精神，他们把集体协作学习作为自我提升的主要方式。对于黑客来说，黑客论坛是一个网络学院，所有的资料可以供具有趋同需求的成员使用、批评和发展。在虚拟社区里，任何新技术、新工具的扩散都会直接影响其他学习者。这种学习模式的基础是一个提出问题，质疑问题，解决问题的集体过程。其核心不在于其个体的成就，更在于学习模式本身。但是，部分黑客论坛通过互联网传播黑客技术，为其他潜在犯罪者提供技术帮助和支持，已经成为亟待解决的问题。

黑客论坛是目前黑客学习平台的主要形式之一。互联网的普及能够使黑客论坛更迅速地被了解、扩散。由于网络黑客论坛具有以上的特点，黑客论坛就是目前网络黑客们的兵工厂、武器库和“启蒙基地”，传授带有恶意攻击性质的黑客技术客观上成为了网络犯罪活动的帮助行为。其对于网络犯罪共具有以下3个促进作用：

- (一) 具有明显教唆性、鼓动性
- (二) 黑客工具普及使网络犯罪门槛进一步降低
- (三) 促进黑客犯罪产业化、专业化、广泛化

二、国内黑客论坛的分类及应对策略

按照内容类型分：

- (1) 正规互联网知识分享类。
- (2) 正规知识、恶意攻击教学混合类。
- (3) 专门用于恶意攻击、破坏性工具发布类。

按照载体分：

- (1) 专门型黑客论坛
(如**免杀网、**安全论坛)
- (2) 寄生于大型技术网站特定版块。
- (3) 兼有论坛、QQ群等通讯群组的复合型平台。

黑客论坛的应对策略

(一) 多措并举，依法规制

(二) 打击前移，打早打小

(三) 加强宣传宣传，创建清朗网络环境

三、我局侦办“黑客论坛”类案件 相关案例介绍

“华中帝国” 非法利用信息网络案

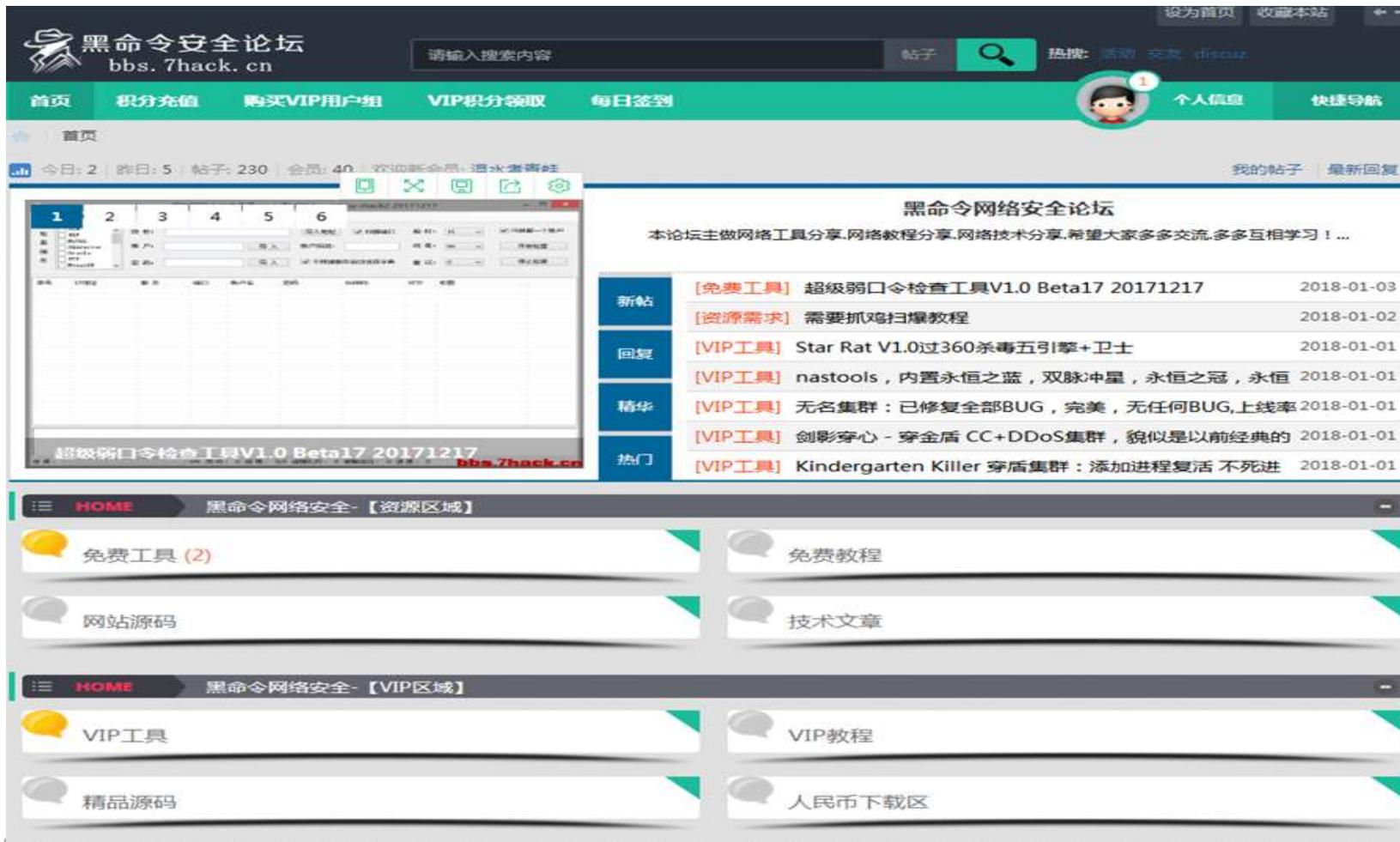


ISC 互联网安全大会



360 互联网安全中心

2018年1月，总队侦查员在梳理涉网犯罪线索时发现一名为“黑命令安全论坛”的网站公开收徒传授黑客犯罪方法并发布大量黑客工具。



黑命令安全论坛

请输入搜索内容

帖子 热搜: [活动](#) [交友](#) [discuz](#)

首页
积分充值
购买VIP用户组
VIP积分领取
每日签到

个人信息

快速导航

首页 > 黑命令网络安全-【资源区域】 > 免费工具

免费工具 今日: 2 ↓ | 主题: 108 | 排名: 1 ↑

★ 收藏本版 | 📧 订阅

发新贴
返回

全部

抓鸡远控 14

渗透工具 56

免杀破解 9

压力测试 8

爆破解密 10

其他工具 11

全部主题 ▾
最新
热门
热帖
精华
更多 ▾

全部主题 ▾	最新	热门	热帖	精华	更多 ▾	■ 新贴	作者	回复/查看	最后发表
🏠 会员价格与特权详细介绍 (新人版) 📄									
📄 版块主题									
							admin	1 32	KuVUGa 2018-3-29 19:55
							admin	3 6	温水煮青蛙 7小时前
							admin	1 4	DDDDDDDDDD DDDD 昨天 18:24
							admin	1 6	ABY空白 3天前
							admin	1 9	Z1j4mW 3天前
							admin	0 7	admin 4天前
							admin	0 1	admin 4天前
							admin	0 3	admin 4天前
							admin	0 4	admin 4天前
							admin	0 2	admin 4天前
							admin	0 2	admin 4天前
							admin	0 1	admin 4天前

黑客工具列表

大家有没有一些弄电话号码的渠道，

【群主】购买论坛VIP找我(654139883) 15:17:13

@全体成员
出售博客VIP

年费/50

永久/100

永久VIP 赠送超值好礼 + 永久技术指导

收徒 价格便宜 包教包会 不存在跑路问题

还差一位 就够5位了

群成员 5/5

- 小北(654139883)
- 培训01(767826751)
- 培训02(2732150445)
- 培训03(2308652512)
- 培训04(2608982626)

【实习】倘若我问心有愧呢? (51565638) 15:29:22

公开收徒传授犯罪方法

小北资源博客 www.7hack.cn

博客首页 | 精品工具 | 精品教程 | VIP专区 | 技术文章 | 网站源码 | 漏洞预警

5tr-045漏洞全自动利用工具，只需要设置...

2017-12-16 0 25

PC QQ9.0版本视觉新UI设计公测版下载

2017-12-4 0 5

Burpsuite1.6破解版-2099年过期

2017-12-4 0 11

傀儡注入点批量扫描工具V6.0

2017-11-30 0 22

HFS2017 破解版 (hfs抓鸡工具)

2017-11-30 2 31

中国斧头WEB管理工具【过狗无后门版】

2017-11-30 0 7

Chopper (中国菜刀) 2014.5.21[经典版...]

2017-11-30 0 7

phpMyAdmin定向爆破工具

2017-11-27 1 6

Test404轻量后台扫描器 V1.5

2017-11-27 0 3

挖蚯蚓V1.1 网站备份批量扫描工具

2017-11-20 3 27

MetinfoSq批量检测工具

2017-11-20 0 6

evilscan - 大规模的IP端口扫描器

2017-11-12 0 11

VIP工具板块

网站特点：不直接参与具体犯罪。而是通过设立网站、通讯群组的方式**传授**犯罪方法，传播黑客工具牟利。经仔细甄别，侦查员发现其进行黑客教学内容则多为传授非法侵入、破坏、控制计算机信息系统，盗取网站数据、控制智能摄像头等实施互联网犯罪的方法手段，甚至通过入侵小网站的方式进行演示。其传播的黑客工具均为新型木马、勒索病毒等**破坏性程序**。

我们认为其行为为触犯了刑法第287条之一“**非法利用信息网络罪**”和刑法285条第三款“**提供侵入、非法控制计算机信息系统程序、工具罪**”。

进一步侦查发现，租住于丰台区华源一里小区的**李某**（男，25岁，吉林省农安县人）疑似为该站站站长。对此，我局立即开展工作。



多次与各级法制部门进行会商

2018年1月，我局对李某实施抓捕，李某对其设立网站传授犯罪方法、提供黑客工具的行为供认不讳。



现场勘验李某电脑



讯问李某

华中帝国 · 论坛

— 资源最多,更新最快! —

请输入搜索内容

论坛 门户 主站 VIP站 应用 积分 申诉 邀请码 举报 免杀演示 积分充值

黑客工具 红客下载 VIP工具 VIP分享 站内交易 投诉举报 游客投稿 会员投稿 骗子公布 站外VIP VIP提问 MD5解密 版规公告 账号申诉 客服QQ 论坛广告 会员守则 官网声明

论坛 > 技术交流

技术交流

	<p>黑客工具</p> <p>远控攻击 每日免杀 综合黑软 黑客必备 加密免杀 脱壳破解 抓鸡扫描 远程攻防 旁注入侵 脚本提权 黑客QQ 腾讯漏洞 软件编程 程序源码 捆绑工具 木马伪装 网马木马 病毒后门</p> <p>版主: 常宇</p>	7872 / 19万
	<p>红客下载</p> <p>绿色工具 破解版 绿色版 注册机 优化版 免注册 单文件 汉化版 绿盟 华彩 热点精选 软件下载 破解版下载 绿色版下载 免费下载 汉化版下载 中文版下载 注册机下载</p>	4859 / 4万
	<p>教程动画</p> <p>技术教程 动画教程 语音教程 视频教程 系列教程 整套教程 学习动画 原创教程 教程种子 千G教程 翻录教程 黑客教程 红客动画 抓鸡教程 免杀教程 入侵教程 破解动画</p>	3391 / 6万
	<p>建站网赚</p> <p>网站建设, 网络赚钱, SEO优化, 安全优化, 广告联盟, 网页制作, 域名注册, 虚拟主机, 网站推广, 网站模板, 百度联盟, 谷歌adsense, 建站源码, 论坛模板, 程序源码, 采集, 网站工具, 淘宝开店</p>	8998 / 6万
	<p>技术文章</p> <p>技术文章, 美文, 全文, 阅读, 大全, 必备, 黑客, 在线, 学习, 破解, 攻击, 脱壳, 远控, 密码, 入侵, 检测, 渗透, 提权, 扫描, 编程</p>	1231 / 1万

据勘查讯问显示, 李某网站上的教程、黑客工具除少量在国外网站购买外, 多数从国内一家名为“华中帝国”的论坛下载, 并称该网站为目前国内设立时间最久、影响最大的黑客网站之一。华中帝国网站随即进入侦查员视野。

- E语言强制锁屏病毒完整源码+模块：密码输入错误，自动摧毁系统 ... 2 3
- 服务器端口检测工具：检测服务器哪些端口可以扫描抓鸡 ... 2 3 4 5 6
- 天眼远程控制软件（破解版）（局域网版）+电脑文件加密软件007，文本加密 ... 2 3 4 5
- 一款很强大的国产渗透工具：集成漏洞扫描，漏洞利用，爆破，入侵等功能 ... 2 3 4 5 6..12
- 小迪web渗透工具包V1.0，最强大的渗透工具合集，压缩后近4G ... 2 3 4 5 6..8
- Memcached DDoS攻击很最近传的很热门，阿里等大型机房都遭受重创！ ... 2 3 4 5 6
- 2018最新免杀下载者木马生成器，大小10k，非常简单
- 2018最新一枚万能无限数量捆绑器，支持任意格式捆绑成一个exe文件运行 ... 2 3 4 5
- memecache-pythonDRDOS攻击脚本带验证，不是网上的泛滥端，采用python编写 ... 2 3 4
- 最强悍的网吧权限破解工具箱：网吧安全性检测工具，网管技术员必备 ... 2 3 4 5 6..8
- 批量getshell 《永不更新版》无任何限制 永久可用！【修复版】 ... 2 3 4 5 6..8
- 免流漏洞利用工具:免流服务器批量getshell+一句话批量执行命令 Linux版 ... 2 3 4 5 6..7
- 缘分最新批量getshell3.0破解版卖200的所谓VIP工具[转自墨客] ... 2 3 4 5 6
- 煤老板V3挖矿工具完整源码+Xmr矿马生成器 /x86/x64通杀/k同行/守护进程/复活 ... 2 3 4 5
- 最新全自动批量getshell工具：支持64种CMS系统！全自动采集URL 自动验证 ... 2 3 4 5 6..9
- Webshell采集管理工具集成一句话爆破+天羽webshell全自动getshell工具 ... 2 3 4 5 6..9
- WiFi万能钥匙解不开的时候还有什么办法？推荐一款Android端WiFi密码破解工具 ... 2 3
- [NET]国外一款免杀捆绑器：Ultimate File Binder ... 2

百万年薪诚招
渗透、数据、社会工程

高价收shell/服务器
点击联系

招聘技术 年薪高达百万
渗透 SEO Q:10446667

长期收购 **联系扣扣**
一手扣扣信封 **68919**

重金收购CP 六合流量
联系 875571111

其他黑客在网站上做广告

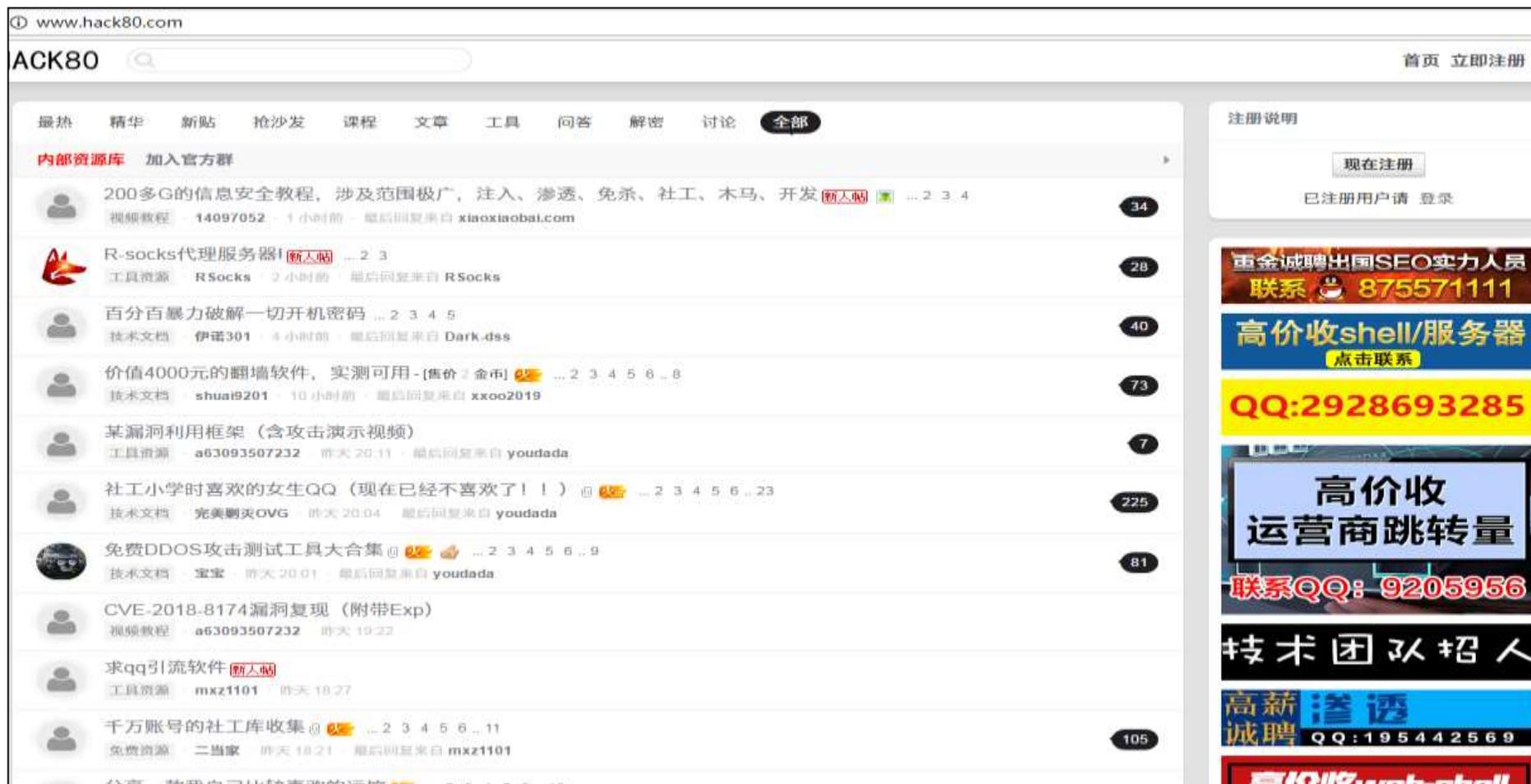
发帖列表



2018年3月，我局将“华中帝国”站长韦某抓获。经勘查，网站中上传的黑客工具和攻击教程达近万个，注册收费会员数千名。经查询相关账目，该人通过发布黑客工具和传授黑客技术非法获利近百万。

The screenshot shows the homepage of the White Ant Security Forum. At the top, there is a navigation bar with the site logo and menu items like '首页', '热门', '看看', '话题', '导航', and '蓝云服务器'. A search bar is also present. The main content area features a large banner for '合作共赢' (Win-Win Cooperation) with the text '加入蚁安会, 获得好资源'. Below this, there are several featured articles and advertisements. One article is titled '【扫描VPS|扫描扫描服务器报价】专业正规可扫可爆服务器'. Another is '2017年VIP王族零基础入门培训系列教程视频导航'. There are also book recommendations like 'Web应用安全攻防' and 'Uday漏洞挖掘技术'. A section titled '最新网络安全资讯' (Latest Network Security News) highlights '海洋CMS (SEACMS) 新版本V6.55补丁仍可被绕过执行任意代码'. On the right, there is a '黑客技术文章' (Hacker Technology Articles) section with a list of 10 items.

2018年6月，关闭违法黑客论坛“白蚁网安”，依法惩处相关涉案人员。



2018年6月，关闭违法黑客论坛“HACK80”，依法惩处相关涉案人员。

开启邀请码注册中，禁止灌水！发现一次永久禁言

拒绝任何人以任何形式在本论坛发表与中华人民共和国法律相抵触的言论！



飞鹰 我的 | 设置 | 消息 | 提醒(4) | 门户管理 | 管理中心 | 退出

银两充值 每日摇摇乐

用户组: 管理员



论坛首页 | 门户首页 | 新人必看 | Vip介绍 | 申请担保 | 社区商店 | 红蓝商城 | 通杀服务器购买

红蓝安全网 - 新手入门指南
常见问题及帮助 - 做任务赚银两
新人报告 - 最常问答 - 银两充值 - 帖子举报

红蓝安全网 - 论坛精华合集
红蓝安全网 - 精华合集 - 速成之路
精品原创 - 加入红蓝vip - Vip工具 - Vip教程

红蓝安全网 - 工具软件
网络教程 - 技术交流 - 程序源码

请输入搜索内容: 帖子 热搜: 红蓝安全网 红蓝客栈 红蓝论坛 爆破防护 linux 社工辅助 破解教程 网赚教程 影视后期 测试教程 C语言编程 服务器 域名拦截 web安全

【站外广告，风险自负】

常年稳定收量《SYN》每天准时结算 支持各种担保（可以走站长担保）

海外全球伪造小包 G/300 电信小包 G/300 移动小包 G/200 海外小包 G/100

《8UC》联系方式: potato:+15075192439 QQ: 326799213

论坛首页 <> 请遵守论坛版规，即日起将随机抽查。发现灌水，广告，骂人，收徒，等内容将.. (2016-2-8)

<p>【官方业务】服务器出租 端口通杀 可扫可爆 全天扫爆 不封机 国内服务器 客服QQ:81071179</p>	<p>【悬赏公告】- 严查灌水，打造一个无水论坛，从即日起，请大家互相监督，发现恶意灌水的，请发帖举报，核实后会给予5-10的银两奖励。</p>	<p>【官方公告】从今日起所有会员发布工具必须到审核板块进行审核，如有违反永久禁言处理！</p>	<p>【招聘招聘】- 招聘各方面给力版主，要求每日发帖不少于3贴，每天在线时间6个小时以上，具体权利和待遇联系QQ:81071179或者在线管理员</p>
<p>【官方业务】- 加入红蓝安全网Vip, 回你日抓干鸡梦, 各种精品教程, 免杀远控, 压力测试等你拿, 期待各位会员的加入, 即可享受众多福利！</p>	<p>【官方公告】1. 发现网盘下载地址失效！可以发帖举报 审核证实后给予奖励10-20银两。 2. 即日起！不管是谁发帖！都不能带QQ群 已及个人QQ。个人网站, 发现后严肃处理。</p>	<p>【官方业务】本站出售免杀远控，单文件免杀远控，过网购过主动，K杀软，过启动拦截，自动加入白名单，肉鸡可找回，稳定。可测试，收代理，购买联系在线客服</p>	<p>【官方公告】论坛所有广告均为商业行为，需要交易的请尽量走担保程序，所有因广告产生的任何纠纷请私下解决</p>
<p>【官方业务】出售台风全套源码带主控1500一套只出售3个需要的速度来购，详细咨询客服 Qq:81071179</p>	<p>【站外广告, 风险自负】天空云DDOS压力测试平台 提供代购海外发包机 提供攻击脚本 联系QQ:3526308115</p>	<p>【站外广告, 风险自负】出售免杀远控 过国内主流杀软 上线无提示 重启上线 可捆绑任意图片或可执行文件, 另出售集群, 挖矿软件 QQ:571601634</p>	<p>【站外广告, 风险自负】出售免杀远控 可捆绑图片文档, 免杀360全套, 管家, 金山, 免杀持久 win7/8/win10系统 QQ: 723200497</p>
<p>【站外广告, 风险自负】全网高价收免杀远控 有的联系 要求过启动 重启上线(360 QQ)骗子与中介勿扰 联系QQ:33410629</p>	<p>【站外广告, 风险自负】出售企业定制版免杀远控, 过360杀毒, 360卫士, QQ管家, 过网购, 免杀持久最少一年, QQ:1150053814</p>	<p>【站外广告, 风险自负】远控 过360 网购 启动 重启上线 长期免杀 秒更新 QQ:2221116133</p>	<p>【站外广告】高价找实力技术, 过启动, 360全套, 管家; , 单文件多文件; 测试后再购买, 可给测试费, 联系QQ:773549130</p>
<p>【官方广告】精品广告位出租80/月详细联系客服</p>	<p>【官方广告】出售精品广告位80/月详细联系客服</p>	<p>【官方广告】精品广告位出租80/月详细联系客服</p>	<p>【官方广告】出售精品广告位80/月详细联系客服</p>

2018年8月，关闭违法黑客论坛“红蓝安全网”，依法惩处相关涉案人员。

四、经验交流

(一) 妥善处理“发展”与“安全”的关系

(二) 加快立法进程，化解网络风险

(三) 动员各界力量构建“网络综合治理体系”



ISC 互联网安全大会



360 互联网安全中心

谢谢!

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

(原“中国互联网安全大会”)