趋势科技新闻稿

[即时发布]

趋势科技发布最新《2013 中国地下市场研究报告》

QQ 群成地下市场主要途径　肉鸡、DDoS 服务、远端存取工具最受欢迎

[趋势科技中国]– [2014 年 10 月 9 日] 黑客犯罪工具在愈发“繁荣”的网络犯罪地下市场所构造的生态环境中，价格越来越低，应用越来越普及，甚至有些产品以免费的方式向犯罪分子提供。因此，洞察网络犯罪地下经济的状况将有助于发现网络犯罪的发展趋势。全球服务器安全、虚拟化安全及云安全领导厂商趋势科技从 2011 年即开始持续监控中国地下市场的动态，并于近日发布了最新的《2013 年中国地下市场研究报告》。报告指出，QQ 群成为地下市场黑客们聚集的主要场所，已入侵的主机、DDoS 服务、远端存取工具是最受欢迎的三种产品与服务，而且移动设备地下市场也快速活跃起来。

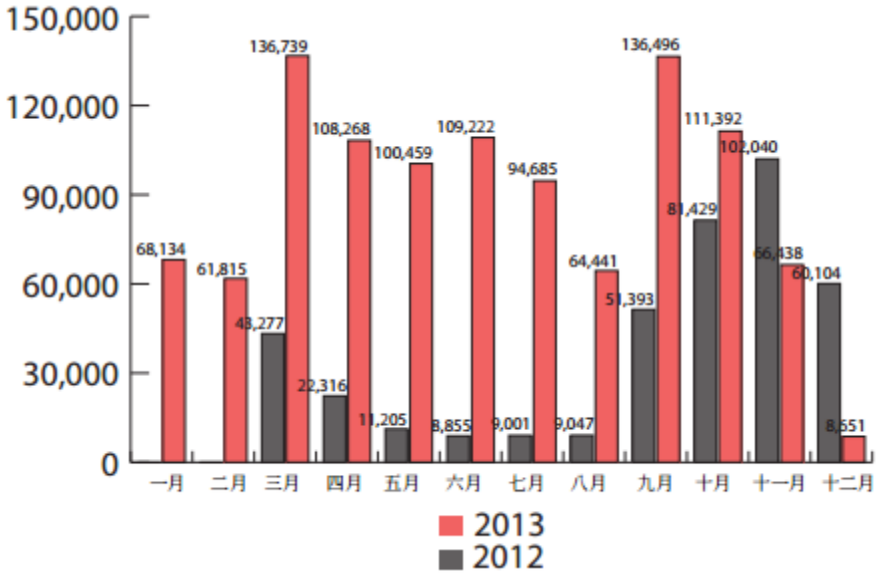
“QQ 群”成为地下市场黑客具体的主要场所

网络犯罪集团利用热门网站服务从事犯罪早已不是新闻，例如今年稍早，Dropbox 和 Evernote 服务就曾遭不发分子用于恶意程序的幕后操纵（Command-and-Control，简称 C&C）通讯。中国境内的网络犯罪亦不例外，他们也利用热门的即时通讯软件 QQ 作为通讯工具。由于 QQ 可以让用户轻松建立多个聊天群，各群之间的信息隐蔽性较好，还能通过群搜索功能快速搜索特定的聊天群，因此 QQ 群现成为地下市场歹徒聚集的主要场所。

【使用关键字“DDoS”搜索 QQ 群的结果】

尽管这里的产品、服务广告刊登时间总是比专业地下论坛或网站的广告来的短，不过，QQ 上的广告却比后者更新更频繁。事实上，利用 QQ 来兜售犯罪软件的网络犯罪集团甚至还建立了一些“地下”专有名词来协助新手找到想要的东西。掌握了地下产品和服务所使用的热门用语之后，我们就能找出需要监控的 QQ 群，进而追踪用户人数最多的群组。

通过对 QQ 群的监控，趋势科技发现，在 2013 年 3 月~12 月期间，经由地下聊天群传输的信息相对于 2012 年同期增长了一倍，聊天成员人数也比 2012 年同期增长约一倍，这显示地下市场活动日趋频繁。



【2012 和 2013 年地下聊天群信息数量比较】

已入侵的主机、DDoS 服务、远端存取工具成为最热门产品

此外，趋势科技也探讨了不同产品及服务在地下市场的热门程度，从中可以了解地下聊天群组的成员最感兴趣的是哪种网络犯罪，地下市场专门用语确实有助于判断每种产品或服务的热门程度。中国地下市场最热门的三项产品与服务分别为：已入侵的主机(是指那些网络犯罪集团可从幕后操纵而其系统拥有者却不知情的主机)、分布式拒绝服务(DDoS)攻击服务以及远程存取工具/木马程序(RAT)。除此之外，还有其他产品与服务可供任何有兴趣者购买。

产品	详细内容	价格
僵尸网络	Windows： • 100 台 Windows XP 僵尸电脑 • 100 台 Windows Server 2003/2008 僵尸电脑 ddos 攻击： • 100 台僵尸电脑 • 300 台僵尸电脑 • 800 台僵尸电脑 • 2,000 台僵尸电脑	8 美元 48 美元 95 美元 208 美元 386 美元 596 美元

漏洞攻击套件	nb 漏洞攻击套件	323 美元
假造帖子/回复/点击/粉丝	百度贴吧： • 100 条新帖子 • 100 条回复 10,000 个“优酷”视频点击 新浪微博： • 100 名粉丝 • 1,000 名粉丝 • 3,000 名粉丝	 16–48 美元 8–16 美元 0.65 美元 2 美元 13 美元 37 美元
假网站	QQ/淘宝/中国工商银行 各种线上游戏 线上游戏交易网站	81 美元 16–32 美元 81–97 美元
扫描的伪造文件	中国/美国/加拿大护照	5 美元
序号/密钥	Microsoft 产品： • Windows® 8 pro • Windows Server 2012 R2 • Microsoft™ office® 2013 pro 其他产品： • Adobe® photoshop® Creative Suite® 6 • AutoCAD® 2013	 0.65–3 美元 0.81–2 美元 0.81–6 美元 0.81–3 美元 3–11 美元
网络流量	每日 500 个 ip 地址 每日 1,000 个 ip 地址 每日 5,000 个 ip 地址 每日 10,000 个 ip 地址 每日 50,000 个 ip 地址 每日 100,000 个 ip 地址 每日 500,000 个 ip 地址	0.26 美元 0.42 美元 2 美元 5 美元 38 美元 95 美元 473 美元
木马程序	QQ 账号窃取程序 淘宝账号窃取程序 云腾银行木马工具套件： • 铜级 • 银级 • 黄金级 • 白金级 • 钻石级	32 美元 323 美元 1,273 美元 1,596 美元 2,080 美元 2,565 美元 3,856 美元

【表：中国地下市场贩卖的产品】

服务	**详细内容**	**价格**
破解	加密 .rar、.zip、.doc、.xls 或 .exe 文件 软件： • dongle 保护 • 注册码 • 用户数量限制保护	45 美元 807–12,919 美元 161 美元 242 美元
专用/防攻击(bulletproof)服务器代管	一个月 (含 DDoS 攻击防护)	81–775 美元
DDoS 攻击	1gb 封包： • syn (每日) • http get (每日)	 16 美元 73 美元

	每日 10gb syn 封包 dns 服务器攻击 DDOS 攻击套件租用： • 一个月 • 六个月 • 一年 • 终生	161 美元 323 美元 81 美元 161 美元 258–323 美元 452–484 美元
伪造文件重制		19 美元
黑客破解	论坛账号： • 一般用户 • 论坛分区管理员 • 论坛管理员 • VIP QQ 账号： • 密码 • 六个月聊天记录 • 一年聊天记录 电子邮件账号： • 个人 • 企业 新浪/微博/人人账号	 81 美元 161 美元 323 美元 官网服务费的 30% 48 美元 81 美元 129 美元 48 美元 81 美元 48 美元
确认恶意程序是否能躲过信息安全软件检查	各种软件	13–19 美元
程序设计	rat 工具套件 木马程序	161 美元 323–8,075 美元
代理（proxy）服务器代管	http socks 代理服务器： • 每月单一固定 ip 地址 • 每月 800 个 ip 地址 • 每月 9,000 个 ip 地址 • 每月 32,000 个 ip 地址	 4 美元 0.16 美元 2 美元 16 美元
rat 工具套件租用	tyt/mbz rat 每年 rd rat： • 一个月 • 一年	97 美元 129 美元 258 美元
散发垃圾邮件	1,000 封垃圾邮件 10,000 封垃圾邮件 20,000 封垃圾邮件 50,000 封垃圾邮件 100,000 封垃圾邮件	13 美元 97 美元 161 美元 323 美元 484 美元
木马程序攻击	每日一个线上游戏	29 美元
VPN 服务器代管	一个月 三个月 一年	3 美元 8–10 美元 19–32 美元

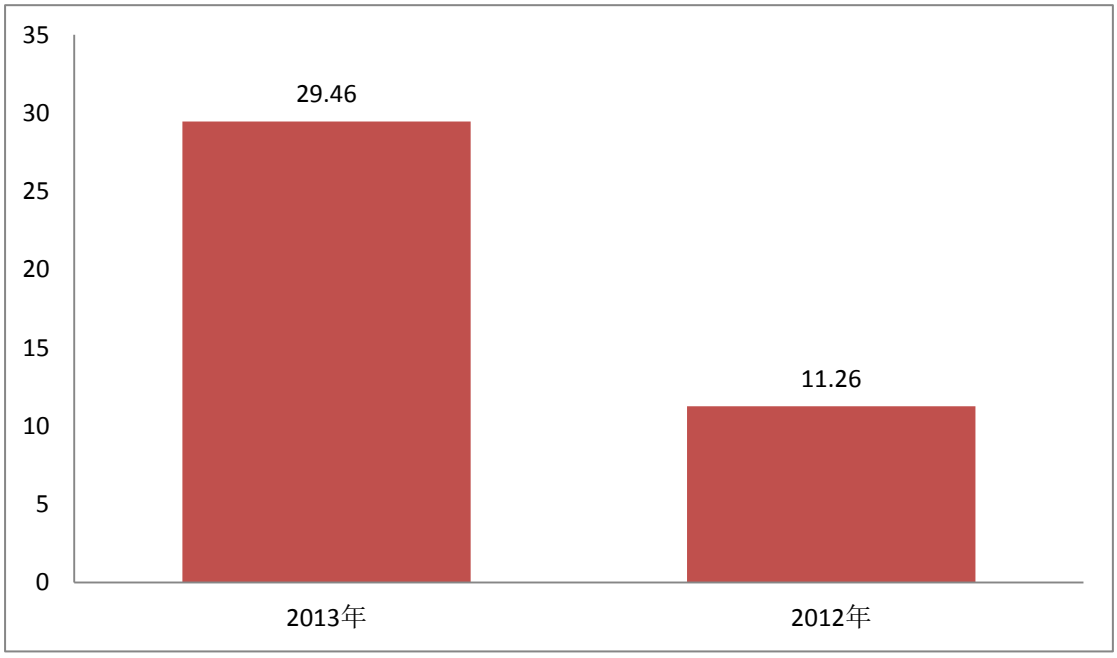
【中国地下市场贩卖的服务】

网络犯罪分子会通过各种方式来入侵用户的主机，并获得主机的控制权，其往往被称为“肉鸡”。他们会在地下市场出售这些“肉鸡”，购买者可以利用这些已入侵的主机来散布恶意程序或垃圾邮件，还可让主机感染可传染给其它相连系统与设备的恶意程序。另外，网路犯罪集团还能操纵大量已入侵的主机发动 DDoS 攻击，在同一时间连上某一个 IP 地址或网址，如此大量的网路流量将瘫痪该网站的服务器。一个新兴的用途是比特币的挖掘，这些“肉鸡”的计算资源会被窃取以用在比特币的挖掘上面。

移动设备地下市场不断活跃

最近几年，针对移动设备的攻击不断快速攀升，这从安卓恶意程序数量的快速成长即可证明。因此，趋势科技也探讨了 2013 年中国新兴移动设备地下市场的状况。

对移动设备地下 QQ 群的监控数据显示，2013 年这些群组的每天平均信息量达到 61.3，非常接近地下市场整体的平均信息量 62.56，这显示其活跃度大增。另外，每一群组每日平均参与成员数量从 2012 年的 11 人左右成长到 2013 年的 29 人左右。也就是说，2013 年每一个移动设备地下聊天群每天大约有 29 名成员参与，几乎是 2012 年的 2.5 倍。



【2013 年与 2012 年移动设备地下聊天群平均成员数量对比】

趋势科技(中国区)业务发展总监童宁指出：“价格不断下滑、功能不断增加，全球的网络地下论坛皆欣欣向荣，尤其是俄罗斯、中国和巴西，这些已成为各国境内黑客贩售产品及服务给网络犯罪集团的热门管道。此外，网络犯罪集团也通过所谓的深层全球网络（Deep Web）来贩售一些全球网络搜索引擎所无法查到的产品和服务，为的就是要让其网络店面不易遭到

执法机关发现及破获。这一切的发展 ,意味着一般大众的计算环境受到攻击的风险越来越高，因此，有必要彻底重新思考安全在日常数字生活当中所应扮演的角色。”

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商 ,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。