KASPERSKY lab

俄罗斯金融网络犯罪活动如何运作

计算机事故调查负责人 Ruslan Stoyanov

ANTIY
安天实验室
技术公益翻译组
非官方中文译本

俄罗斯金融网络犯罪活动如何运作

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Russian Financial Cybercrime: How It Works		
原文作者	Ruslan Stoyanov	**原文发布日期**	2015 年 11 月 19 日
作者简介	Ruslan Stoyanov 是卡巴斯基实验室计算机事故调查负责人。		
原文发布单位	卡巴斯基实验室		
原文出处	https://securelist.com/files/2015/11/Kaspersky_Lab_cybercrime_underground_report_eng_v1_0.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

目录

简介

俄罗斯网络犯罪市场闻名全球。在本文中，我们所说的“俄罗斯犯罪市场”是指拥有俄罗斯联邦国籍或前苏联国家（主要是乌克兰和波罗的海）国籍的网络犯罪分子。为什么这个市场享誉全球？主要有两个因素：首先是全球媒体频繁地报道俄罗斯网络犯罪活动。其次，为了实现交易，俄罗斯网络犯罪社区开放了在线平台，宣传其各种“服务”和“产品”，并讨论它们的质量和应用方法。

随着时间的推移，这个地下市场的“产品”和“服务”范围不断演变，越来越专注于金融攻击，而且也越来越复杂。其中一个最常见的网络犯罪类型是（现在仍然是）窃取支付卡数据。随着网上商店和其他电子支付交易的出现，DDoS 攻击和网络金融犯罪活动越来越流行，诈骗者的主要目标是用户的支付数据，或者直接从用户账户/企业账户中窃取资金。

2006 年，用户和企业的电子钱包攻击首次遭到木马 ibank 的攻击；随后而来的是 ZeuS（2007 年）和 SpyEye（2009 年），其次 Carberp 组织（2010 年）和 Carbanak 组织（2013 年）。这还不是完整的名单；犯罪分子还会利用其他木马来窃取用户的资金和数据。

随着网络金融交易越来越普遍，支持这种操作的企业对网络犯罪分子来说越来越具有吸引力。在过去的几年里，网络犯罪分子不仅攻击银行和网上商店的客户，还会直接利用银行和支付系统。Carbanak 网络攻击组织专注于攻击银行，今年早些时候，卡巴斯基实验室披露了该组织的攻击活动，该案例证明了这种趋势。

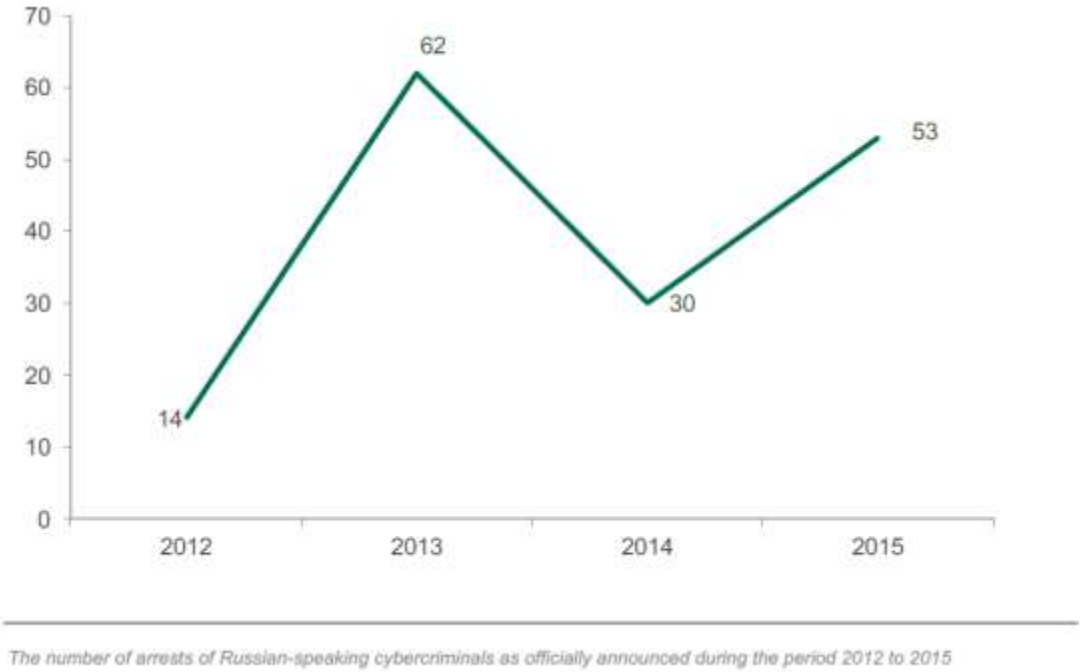
自俄罗斯地下黑客市场出现以来，卡巴斯基实验室的专家们就一直对其进行监控。卡巴斯基实验室定期发布金融网络威胁报告，追踪金融恶意软件的数量变化情况。攻击数量的信息能够反映该问题的严重程度，但并没有透露谁创造了它们以及攻击者如何执行活动。我们希望我们的审查有助于揭示金融网络犯罪的情况。

本文中给出的数据是卡巴斯基实验室的专家们在过去的几年中对俄罗斯网络犯罪市场进行了几十次调查而获取的。

情况综述

根据卡巴斯基实验室的研究，2012 年到 2015 年之间，各个国家（包括美国、俄罗斯、白俄罗斯、乌克兰和欧盟）的执法机构逮捕了超过 160 名俄罗斯网络犯罪分子，他们分别是大中小型犯罪组织的成员。他们涉嫌利用恶意软件窃取资金。他们在世界各地活动，导致的损失总额超过 7.9 亿美元（该数据根据 2012 年-2015 年间的金融犯罪活动分析和卡巴斯基

实验室的数据得出）。其中，约 5.09 亿美元来自非前苏联国家。当然，这个数字只包括已经确认的损失，详细信息是执法机关在调查过程中获得的。实际上，网络犯罪分子窃取的资金可能远多于此。



被逮捕的俄罗斯网络犯罪分子的数量（2012 年-2015 年）

自 2013 年，卡巴斯基实验室的计算机事件调查小组已经参与了超过 330 起网络安全事件的调查。其中，超过 95%的案件涉及资金或财务信息的失窃。

虽然，与 2014 年相比，2015 年被逮捕的俄罗斯网络犯罪分子数量显著增加，但网络罪犯市场还是“人满为患”。根据卡巴斯基实验室专家们的研究，在过去的三年中，俄罗斯网络犯罪分子已经增加到 1000 人。有的人负责创建基础设施，有的人负责编写和传播恶意代码，有的人负责窃取资金或兑现赃款。不过，大多数被捕者都还没被投进监狱。

我们可以相当准确地计算出一个活跃的犯罪组织的核心成员的数量：组织人员、负责从被感染账户取钱的资金流管理人员、专业黑客。在整个网络犯罪地下市场中，只有约 20 名这样的核心人员。他们会定期访问地下论坛，卡巴斯基实验室的专家们获得了大量的有用信息，表明这 20 个人在网络资金和信息窃取活动中发挥着主要作用。

在俄罗斯及其邻国实施网络犯罪活动的组织的确切数量尚不清楚 很多组织进行了几次窃取活动，然后，出于各种原因停止了活动。一些已知的组织解体后，其成员会加入新的犯罪组织。

卡巴斯基实验室的计算机事件调查部门现在可以确认，至少有 5 个主要的网络犯罪组织专门从事金融犯罪活动。在过去的几年中，卡巴斯基实验室的专家们一直在对其进行监控。

2012 年-2013 年期间，卡巴斯基实验室的专家们发现了这 5 个组织，现在他们仍然活跃。每个组织的成员介于 10 到 40 人。其中，至少有 2 个组织不仅攻击俄罗斯境内的目标，还攻击美国、英国、澳大利亚、法国、意大利和德国的目标。

由于对这些组织的调查还未完成，因此我们无法发布更详细的信息。卡巴斯基实验室会继续调查他们的活动，并与俄罗斯和其他国家的执法机构协作，以遏制他们的网络犯罪业务。

通过调查这些组织的活动，卡巴斯基实验室专家了解了他们的行动方法和网络犯罪市场的结构。

俄罗斯网络犯罪市场的结构

“各种产品和服务”

在网络犯罪市场中，通常有各种各样的“服务”和“产品”，用于网络空间中的各种非法行动。这些“产品”和“服务”通过专门的在线论坛提供给用户，大部分这类论坛不对其他人开发。

这些“产品”包括：

- 未经授权地访问计算机或移动设备的软件，旨在从被感染设备中窃取数据或从受害者账户中窃取资金（木马）；
- 利用受害者计算机上软件漏洞的软件（漏洞利用代码）；
- 窃取的信用卡数据库和其他有价值的信息；
- 网络流量（特定用户访问客户要求的网站的次数）。

这些“服务”包括：

- 传播垃圾邮件；
- 组织 DDoS 攻击（利用请求导致网站过载，使合法用户无法访问该网站）；
- 检测恶意软件能否绕过反病毒检测；
- 恶意软件“加壳”（使用特殊软件[加壳器]改变恶意软件，使其不被杀毒软件检测到）；
- 出租漏洞利用包；
- 出租专用服务器；
- VPN（匿名访问 web 资源，保护数据交换）；
- 出租防滥用托管服务（托管不会响应对恶意内容的投诉，因此不会禁用服务器）；
- 出租僵尸网络；
- 评估窃取的信用卡数据；
- 数据验证服务（虚假通话，虚假文件扫描）；
- 提高恶意广告网站在搜索结果中的排名（Black SEO）；
- 购买“产品”和“服务”的中介；
- 取钱和套现。

在网络犯罪市场中，一般是通过电子支付系统来购买“产品”和“服务”的，例如 WebMoney、Perfect Money、Bitcoin 等。

所有这些“产品”和“服务”可以以各种组合进行销售，这主要是为了进行 4 类犯罪活动。不同类型的犯罪活动也可以以各种方式进行组合，这取决于犯罪组织。

- DDoS 攻击（用于勒索）；
- 窃取个人信息和数据，从而访问电子货币（转售这些数据或窃取资金）；
- 从银行或其他企业的账户中窃取资金；
- 国内或企业间谍活动；
- 阻断对受感染计算机上数据的访问，从而进行勒索。

根据卡巴斯基实验室专家们的研究，目前最常见的犯罪类型是窃取资金。因此，本报告的其余部分将主要关注这一领域。

金融网络犯罪“劳动力市场”

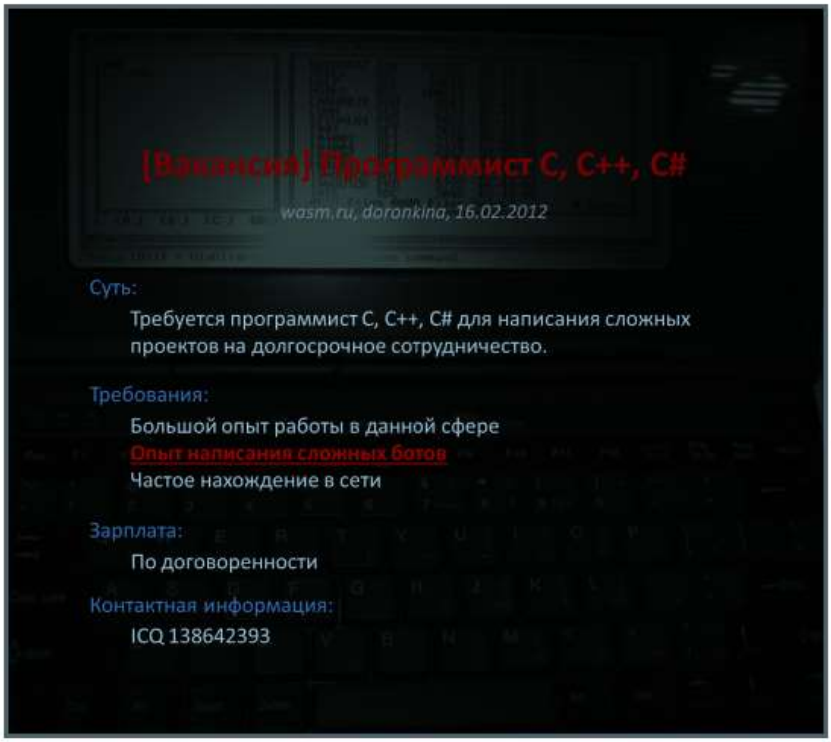
创建“产品”和提供“服务”需要各种技术，这导致专业人员劳动力市场参与金融网络犯罪活动。

在任何 IT 相关的公司中，都会需要以下关键角色：

- 编程人员/编码人员/病毒作者（创建新的恶意软件和修改现有的恶意软件）；
- 网页设计人员（创建网络钓鱼页面、电子邮件等）；
- 系统管理员（创建和支持 IT 基础设施）；
- 测试人员（测试恶意软件）；
- “加密人员”（负责为恶意代码加壳，以绕过反病毒检测）。

上述名单中没有犯罪组织的负责人、资金流管理人员和负责套现的钱骡管理人。这是因为，这些人之间的关系不是雇主与雇员，更多的是合作伙伴关系。

根据犯罪活动的类型和程度，犯罪组织的负责人或者聘用“人员”，并向他们支付固定薪资；或者与自由职业者合作，根据项目支付薪资。



An offer of employment posted on a semi-closed forum inviting a programmer to join a cybercriminal group. The job requirements include experience in writing complex bots.

“员工”要么通过传统网站（参与网络犯罪活动的人在此聚集）招募，要么通过有兴趣在网上赚钱的人士的非常规资源招募。在某些情况下，这些广告被放置在主流求职网站上，或远程进行劳动力交换。

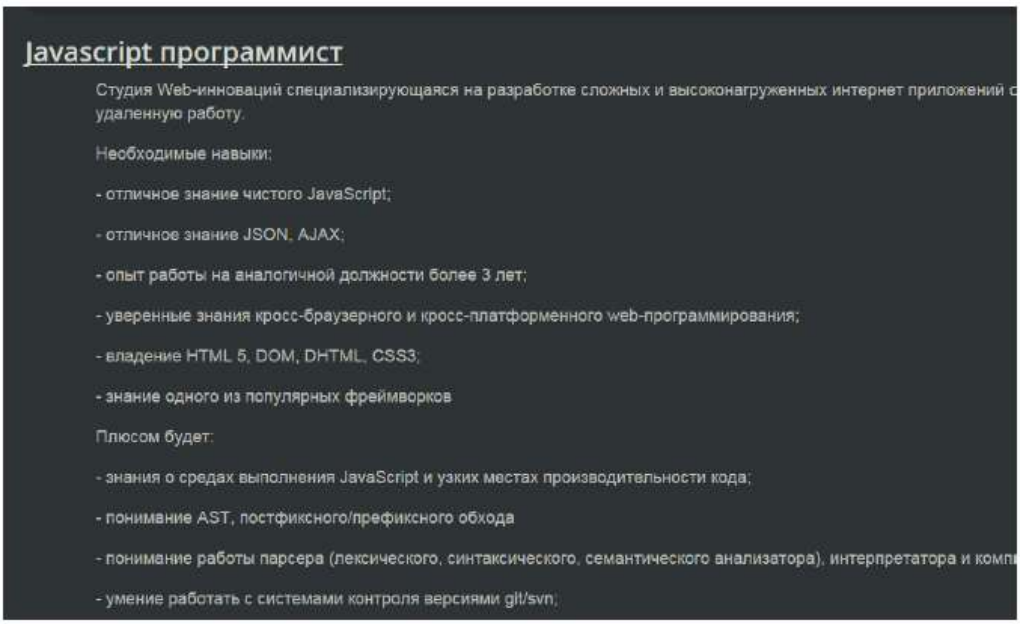
总的来说，参与网络犯罪活动的员工可以分为两类：一类知道自己从事的项目不合法；一类则不知道项目不合法（至少在开始时是这样）。在后一种情况下，这些人通常负责执行相对简单的操作，如复制银行系统和网站的界面。

通过广告“真实”的职位空缺，网络犯罪分子往往希望从俄罗斯及周边国家（主要是乌克兰）的偏远地区招募员工，在这些地方，IT 人员面临相当严重的就业和薪水问题。

A fraudster has advertised a job vacancy for java / flash specialists on a popular Ukrainian website. The job requirements include a good level of programming skills in Java, Flash, knowledge of JVM / AVM specifications, and others. The organizer offers remote work and full employment with a salary of $2,500.

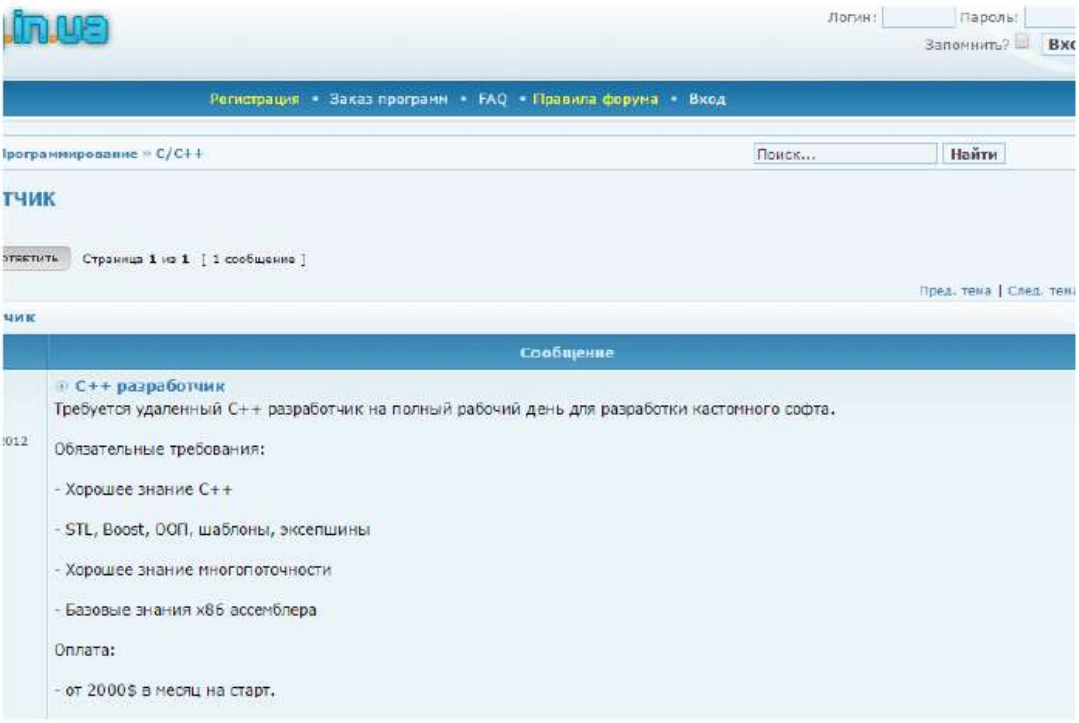
在这些地区寻找“员工”的原因很简单：相比于大城市的员工，这样更省钱。而且，犯罪分子还经常优先考虑以前没有参与过网络犯罪活动的候选人。

通常情况下，这样的工作机会都显示为合法。但是一旦接收到任务，就会弄清楚真正的目的。



在这个例子中，犯罪组织的组织者提供了一个 javascript 程序员的职位，自称是一家从事高级互联网应用开发的 Web 创新工作室。

在非法求职网站的情况下，经验不足的用户就会上当。



This vacancy invites a C ++ developer to develop "custom" software. In this context "custom" software means malicious software.

该职位邀请一名 C++开发人员来开发“定制”软件。这里的“定制”软件指的就是恶意软件。

雇用偏远地区“员工”的第二个原因是：组织者希望尽可能地保证活动的匿名性，并确保任何承包商都无法获得该组织的完整信息。

成立犯罪组织的选择

就成员数量和活动范围上来说，参与窃取资金或财务信息的犯罪组织有很大的不同。主要有 3 种类型：

- 联盟项目
- 独立的经销商，中小型组织（最多 10 个成员）
- 大型有组织的团伙（10 个或更多的成员）

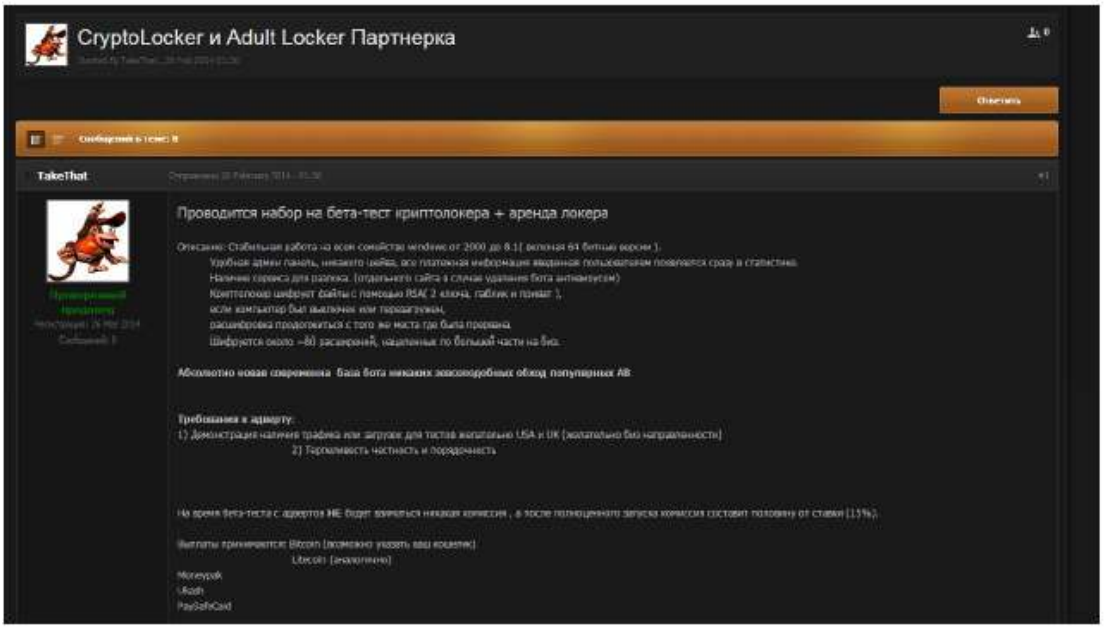
这样的区分有名无实。各组织的活动规模取决于成员的水平、野心和组织能力。在某些案例中，卡巴斯基实验室专家们发现，相对较小的犯罪组织也会执行通常需要更多人员的项目。

联属项目

联属项目是参与网络犯罪活动最容易和最经济的方法。联属项目的出发点是，组织者向其“附属”提供网络犯罪活动所需的工具。这些“附属”的任务是尽可能多地用木马感染目标。产生尽可能多的成功的恶意软件感染的可能。作为回报，联属项目的所有者根据感染结果与这些附属分享收入。根据欺诈方案的类型，可以分享的包括：

- 从网银用户的账户中窃取的资金总数；
- 网络犯罪分子使用勒索木马获得的赎金；
- 利用恶意程序，向移动付费号码发送短信，从移动设备用户的“预付费”账户中窃取资金。

创建和支持以窃取资金为目的的联属项目是一种网络犯罪活动。然而，这样的项目往往由大型有组织团伙实施，我们稍后介绍其活动。



卡巴斯基实验室的专家表示，联属项目越来越受俄罗斯网络犯罪分子的欢迎。其流行的主要驱动力是 可以用恶意程序感染用户的移动设备 然后向移动付费号码发送短信。然而，2014 年春，俄罗斯监管机构对推出此类服务的企业提出了新要求，其中包括：购买收费服务时，需要用户再次确认。这种变化有助于减少恶意程序的数量，几乎到了零。然而，有些组织仍然利用联属网络犯罪活动来传播勒索软件。

小型团伙

这种形式的网络犯罪活动和联署项目的区别在于，在这种情况下，犯罪分子或犯罪组织自己组织其诈骗计划。攻击活动所需的大多数工具，如恶意软件、修改后的恶意软件（“重

新包装”的恶意软件）、流量、服务器等，都从黑市上购买。通常情况下，这些组织的成员不是计算机和网络技术领域的专家；他们通过公共资源，通常是论坛，来了解金融攻击活动需要的组件。这类组织的能力也受到许多因素的限制。特别是，广泛使用的恶意软件导致安全解决方案能很快地检测到它们。反过来，这使得网络罪犯在恶意软件传播和“重新包装”上投入更多的资金，以绕过检测。最终的结果是：攻击者获得的利润显著下降。

这类网络犯罪分子一旦犯错，就会导致身份暴露或被捕。然而，由于参与网络犯罪活动的成本相对较低（200 美元起），这种“业余”的犯罪形式也颇具吸引力。

2012 年，俄罗斯法院审判了这样一个“业余”犯罪组织，指控他们从一家俄罗斯银行的客户网银账户中窃取了 1300 万卢布（价值约 42.2 万美元）。卡巴斯基实验室的专家们经过全面排查，收集了大量帮助执法部门识别攻击者身份的信息。

法院判处其中两名成员 4 年和半年的有期徒刑。然而，这一判决并没有阻止犯罪分子们。他们继续作案，在接下来的两年半的时间里，他们又通过犯罪活动窃取了大量资金。2015 年 5 月，他们再次被捕。

大型有组织的犯罪团伙

大型犯罪团伙不同于其他的犯罪组织，包括更大的活动的规模、更全面的组织和行动方法。这样的团伙可能有几十个成员（不包括用于套现和“洗钱”的钱骡）。他们的攻击目标不局限于网银客户，他们还会攻击中小型企业。其中最大和最复杂的组织，如 Carbanak，主要针对银行和电子支付系统。

大型团伙的业务结构与较小的团伙显著不同。在一定程度上，从事软件开发的一般规模的企业也是这种结构。

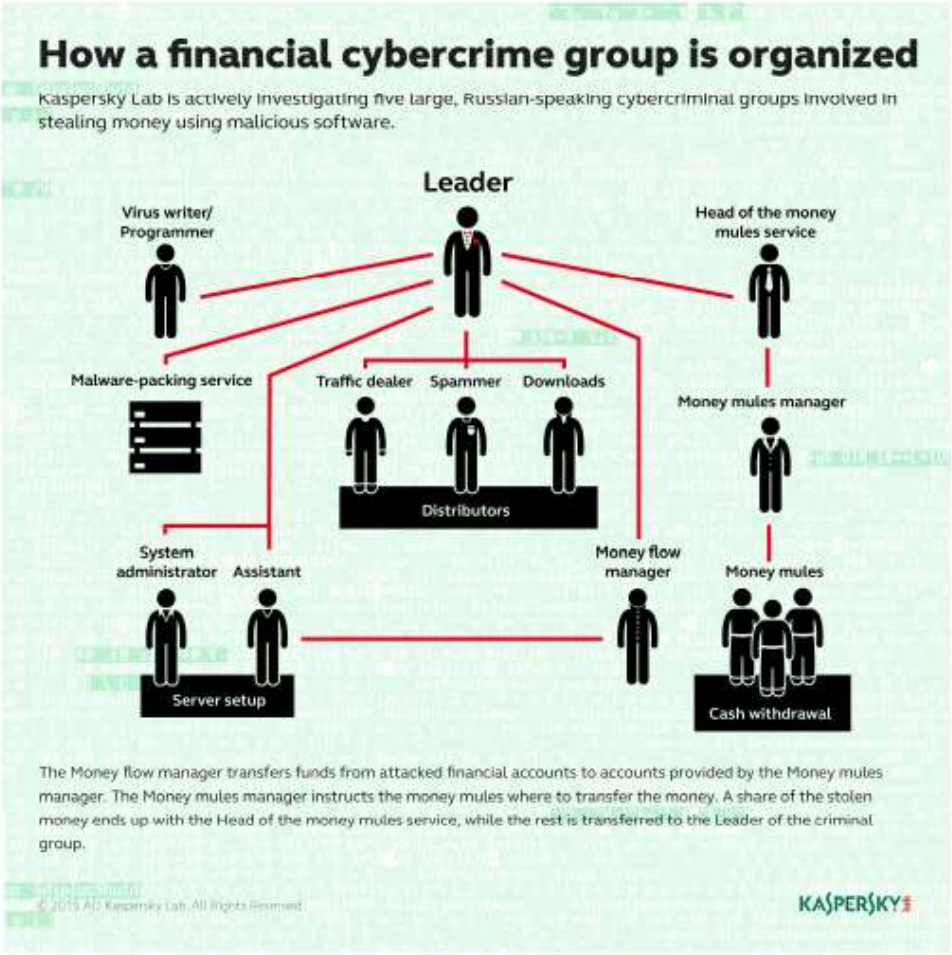
特别是，大型团伙有某种形式的正规工作人员，他们定期领取薪资，执行任务。然而，即使在这些大型的专业团伙中，有些任务会交由第三方承包商。例如，恶意软件的“重新包装”可以由自己的工作人员完成，也有可能雇佣病毒作者或经由第三方服务（在特殊软件的帮助下自动完成）。。对于犯罪活动所需要的其他 IT 基础设施元素来说，这一点是相同的。

此类大型有组织犯罪团伙包括 Carberp 组织，其成员在 2012 年和 2013 年分别在俄罗斯和乌克兰被捕。2015 年初，卡巴斯基实验室还披露了 Carbanak 组织。

虽然，合作伙伴项目和小团体活动也会导致数十万美元的损失，但是大型犯罪团伙是最危险的和最具破坏性的。Carberp 造成的损害估计达到数亿美元（甚至达到 10 亿美元）。在这方面，研究这些团伙的能力和战略是非常重要的，这样我们能够更有效地调查他们的活动并最终进行压制。

大型网络犯罪团伙中的角色分配

犯罪"专家"实施的金融网络犯罪活动 ,能够给安全和金融部门造成数百万美元的损失。通常，这样的犯罪活动需要准备好几个月。这种准备包括创建复杂的基础设施、选择和开发恶意软件、全面研究目标从而明确目标的内部运行和安全漏洞。犯罪团伙的每个成员都有自己的任务。



The composition of middle-sized and large criminal groups

在参与资金窃取的犯罪组织种，都包括以下角色。从事其他犯罪活动的组织可能需要不同的角色。

病毒作者/编程人员

病毒作者或编程人员负责创建恶意程序 ,这种恶意程序允许攻击者在目标企业的网络中创建据点，下载更多的恶意软件，这将有助于他们获得所需的信息，并最终窃取资金。

在各个组织种，成员的重要性和他们与组织者的关系的也是不同的。例如，如果一个组

织使用现成的恶意软件或从病毒作者购买的恶意软件，他们的能力就会受到限制。他们通过设置和修改恶意程序使其在基础设施上运作，从事一种特定的网络犯罪活动，或者是通过修改恶意软件来攻击某一类机构。然而，最先进的团伙往往依靠自己的“开发”，因为这样能够使使恶意程序不太明显，避免被最安全的解决方案检测到，并提供了更多的恶意软件修改机会。如果是这种情况下，病毒作者的作用就会更加重要，因为它们负责恶意程序的架构和功能集。

病毒作者还可能负责恶意软件的“重新包装”。但是，只有当组织者希望保持任务数量最大，或者原始软件旨在进行恶意软件“重新包装”时，这种情况才会出现。在大多数情况下，这一过程会被转移给第三方承包商或通过包装访问实现。

测试人员

在犯罪团伙中，测试人员的作用与合法 IT 企业中的测试人员没有太大的差别。在这两种情况下，测试人员从管理人员手中获得不同环境中（不同操作系统版本，不同的应用程序安装等）的程序测试规范并执行。如果诈骗方案涉及虚假的远程银行或电子支付系统界面，测试人员的任务也包监控这些虚假活动的正确运行。

网页设计人员和编程人员

通常情况下，网页设计人员和编程人员都是远程办公的，其任务包括创建网络钓鱼页面、钓鱼网站、虚假的应用程序界面和 web 注入。所有这些都是为了窃取数据，以入侵电子支付和电子银行系统。

传播人员

传播人员的目的是：确保恶意软件被尽可能多的设备下载，可以使用多种工具来实现。通常，组织者确定需要被感染的用户，并从流量提供商（他们提供的服务吸引用户访问特定的网站）购买所需类型的流量。

An advert offering to buy traffic. Cybercriminals are willing to pay only for the successful installation of malicious software at $ 140 per 1000 "call-backs" (a message that is sent by the malware to the command server after a successful infection).

一则购买流量的广告。只要成功安装了恶意软件，每 1000 条“回调”（成功感染后，木马发送给 C&C 服务器的一条信息），犯罪分子就会支付 140 美元。

组织者可以选择和订购垃圾邮件，邮件中包含将受感染的附件文件或恶意网站的链接。组织者也可以选择目标常常访问的网站；使黑客入侵网站并植入漏洞利用包。当然，所有这些工具都可以彼此组合使用。

黑客

通常情况下，在攻击过程中，组织者拥有的漏洞利用代码和恶意软件不足以攻击所有目标计算机，可能有必要入侵特定的计算机或网站。在这种情况下，组织者会安排黑客（拥有信息安全技术并能够进行非标准任务）执行任务。在卡巴斯基实验室的专家审查的很多案例中，黑客偶尔参与任务，并根据服务收取费用。然而，如果需要定期进行黑客活动（例如，针对金融机构的攻击），黑客就会成为一个“团队成员”。通常，这名黑客会成为组织的关键成员，如组织者和资金流管理人员。

系统管理员

网络犯罪组织的系统管理员与合法公司的系统管理员执行几乎相同的任务 :他们实施和维护 IT 基础设施。网络犯罪组织的系统管理员会配置管理服务器，为服务器购买防滥用托管服务，确保工具能够匿名连接到服务器（VPN）并解决其他的技术挑战，包括与雇用的远程系统管理员交互以执行小型任务。

电话服务

社会工程手段对网络犯罪分子业务的成功至关重要 ,尤其是当涉及窃取企业的巨额资金时。在大多数情况下，即使攻击者能够控制用于交易的计算机，但是还要确认其合法性才能成功完成操作。这就是“电话服务”的目的所在。在指定的时间，犯罪组织的“员工”伪装为受攻击企业或银行的工作人员，并确认交易的合法性。

“电话服务”可以作为犯罪组织的一部分或作为第三方机构，参与特定的网络犯罪活动并收取费用。在犯罪分子相互通信的论坛上，会有大量提供此类服务的广告。

这则广告提供英语、德语、荷兰语和法语的“电话服务”。该组织专门给网络商店、银行以及受骗者打电话。此外，该组织还能够快速创建本地免费电话号码，伪装为支持服务（接收短信、接收和发送传真）。每次通话，犯罪分子收费 10 至 12 美元，接收短信收费 10 美元，创建免费电话号码收费 15 美元。

卡巴斯基实验室表示，大型网络犯罪组织设立自己的“电话服务”，所以他们很少求助于第三方提供商。

资金流管理人员

在网络犯罪组织中，当所有的技术任务（选择和感染目标，在其基础设施中确定目标）完成，且盗窃准备做好后，资金流向管理人员就要发挥作用了。资金流管理人员负责把资金从受感染账户中取出来。然而，他们不仅仅是下命令，而是在整个过程中都扮演关键角色。

资金流管理人员很了解目标企业的内部情况（他们甚至知道目标企业员工的午餐时间，并在他们离开的时间进行转账）。他们知道自动反欺诈系统如何运作，以及如何绕过它们。换句话说 ,除了当盗贼 ,资金流管理人员还能执行“专家”任务或不可能实现自动化的任务。或许是因为这个特殊的身份，资金流管理人员是犯罪组织中不多的几个按百分比拿钱的成

员，而不是领取固定“薪资”。

资金流管理人员还经常操作僵尸网络 将从被感染计算机中获得的信息进行分析和分类（访问远程银行服务、了解账户中的可用资金、确定受感染的计算机术语哪个企业，等等）。

除了钱骡，这些“工作条件”仅由骡子项目的领导共享。

骡子头（骡子“项目”负责人）

在犯罪组织种，骡子头与窃取资金的人密切合作。骡子的功能是获取赃款，取现并向犯罪组织转移应有的份额。要做到这一点，骡子头需要建立自己的基础设施，包括合法实体的账户和他们自己的账户，将窃取的资金转移到自己的账户中，然后转移到骗子手中。骡子项目负责人与犯罪团伙的组织者协作，并为他们提供特定的赃款。根据卡巴斯基实验室获得的信息，骡子项目负责人和资金流管理人员获取的佣金可以达到被盗资金的一半之多。

骡子“项目”

在任何金融网络犯罪活动中，骡子项目都是一个重要组成部分。这类组织包括一个或多个组织者，以及多达几十个骡子。

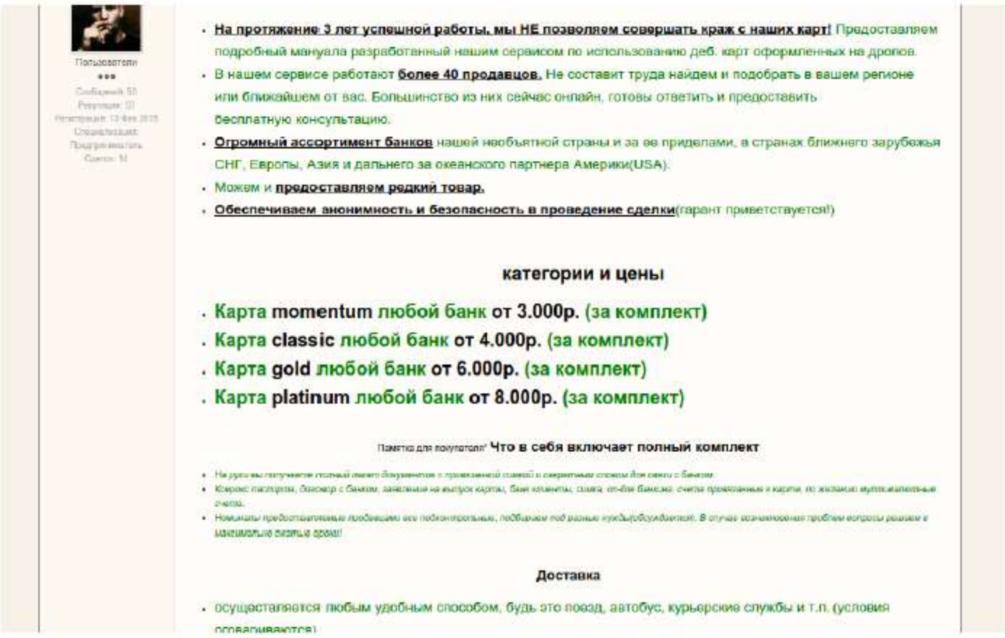
骡子是各种支付方式的持有者，听从钱骡管理人的命令，负责把自己账户中的钱取出现金，或转账给钱骡管理人指定的账户。

骡子可分为两种类型：被骗的和知情的。被骗的骡子至少在刚开始与钱骡管理人合作时并没有意识到参与了犯罪活动。一般来讲 ,他们在取现和转账时会收到一些似是而非的借口。例如，钱骡管理人可以建立一个合法实体，并任命一个管理人（如财务总监），负责执行被骗骡子的功能（如签署企业文件），事实上，这是取赃款的合法掩护。

知情骡子对钱骡管理人的真正意图了如指掌。

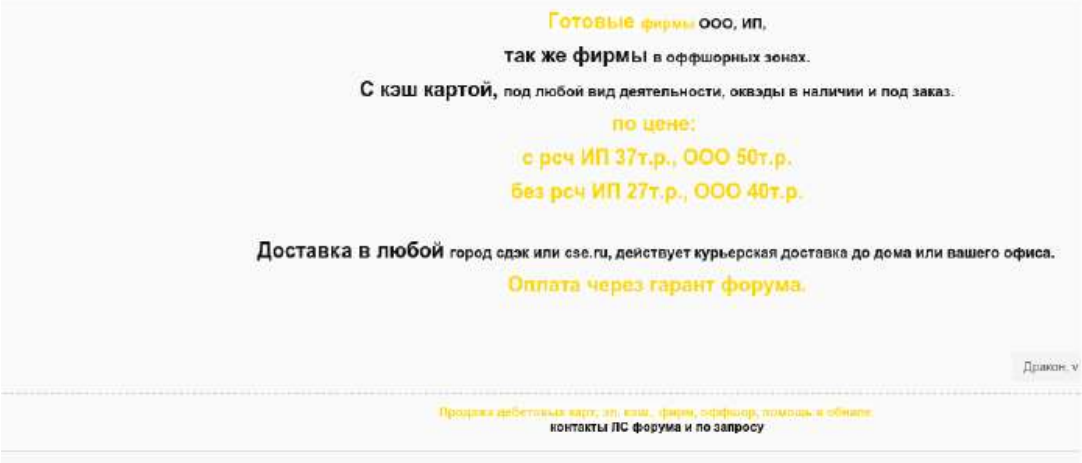
骡子项目有多种取钱方法。根据资金被盗的数量，他们可能通过个人信用卡来套现，并从钱骡管理人那里赚一小笔钱，或通过合法实体，在企业银行账户上办理“工资项目”（给企业员工发工资）。

但是，另一种常用的方法是让知情骡子在不同的银行开设几十个账户。



此广告提供可以取现的支付卡（卡片、授权文件、与该银行账户关联的 SIM 卡）。在售的卡包括俄罗斯银行、邻国银行、欧洲、亚洲和美国银行发行的各种卡。动力卡的成本是 3000 卢布（少于 50 美元），白金卡 8000 卢布（约 120 美元）。

当盗窃活动发生在俄罗斯境外时，知情骡子的角色由东欧国家的人民来扮演，这些人需要短时间地在几个国家之间穿行，用自己的名字开设银行账户。之后，知情骡子会把访问这些账户所需的数据提供给钱骡管理人。之后，这些账户就会被用于取钱。



这则广告销售在俄罗斯联邦注册并位于海岸周边的公司名单。网络犯罪分子的服务费为 560 到 750 美元。

商人

商人（stuffer）一词来自单词“stuff”（意思是“商品”）。一种取现方式是通过在线购买商品然后再转卖，给欺诈者相应的酬金。完成这项任务的就是商人，他们负责用受害者账户中的钱网上购买商品。

事实上，商人是资金流管理人的一种变形。如果窃取到的金额较少，才会通过在线购买商品的方式取现。一般来说，商人都以小组形式合作。这种“合作”通常购买特定类型的商品，有时来自特定的制造商或有明确的型号。

组织者

如果我们把网络犯罪活动看作一个项目，组织者就是犯罪团伙的总经理。他们的职责通常包括：为准备阶段提供资金，为执行者分配任务，监控执行人的表现，联系第三方机构，如骡子项目和电话服务（如过该组织自己没有）。组织者会确定攻击目标，选择所需的“专家”，并与其协商解决。

攻击阶段

应当指出的是，上述分类不是一成不变的。在一些情况下，组织中的某个成员可以身兼数职。不过，不管有多少人执行任务，每个人的角色都如我们所介绍的那样。下面，我们介绍下他们的“实时”工作情况。

1. **探索。**当涉及到以特定公司为目标的针对性攻击时，组织者首先会要求承包商收集

关于这个公司的信息，这将有助于开发用于第一阶段攻击的社会工程方案。如果我们谈论的是针对个人用户的攻击，就会跳过初步探索阶段，或限制性地选择“目标受众”（例如，某家银行的网银用户），创建网络钓鱼电子邮件和钓鱼网站。

2. 感染。通过执行钓鱼攻击或发送包含恶意附件/恶意网页链接的钓鱼邮件来渗透企业网络。只要用户打开附件或点击链接，就会被恶意软件感染。通常情况下，感染是自动发生的，无需用户的意识和参与。点击链接后，恶意程序会自动下载用户的计算机上（挂马）并运行。

在其他情况下，攻击者入侵流行的网站，在网站上植入工具，把用户重定向到包含漏洞的第三方网站。一旦进入了这个网站，用户就会感染恶意软件。

一旦进入系统内部，网络犯罪分子就会利用多种恶意工具，以巩固他们的存在。例如，，当企业的安全软件删除了先前版本的恶意软件后，受感染企业的内部网络还会重新安装恶意软件。此外，攻击者往往设置了企业的基础设施软件，从而从外部方便地访问公司内部网络。

3. 探索和实施。远程管理程序会下载到受攻击的计算机上。网络犯罪分子会利用这些程序获取系统的管理员凭证。许多用户都知道合法的远程管理程序也会用到这一点

4. 窃取资金。在最后阶段，网络犯罪分子会登陆目标企业的财务系统，把账户中的资金转移给骡子项目账户，或者直接从 ATM 上取钱。

结论

最近几年，越来越多的俄罗斯犯罪分子开始从事金融犯罪活动，造成这一增长的原因有很多。主要有：

- 执法机构没有足够的合格人员；
- 立法不足，导致犯罪分子能够逃避责任或者减轻处罚；
- 不同国家的执法机构和专业组织之间缺乏合作。

不像现实世界中，网络空间中的抢劫常常被人忽视，而且收集数字证据的机会也很少。此外，犯罪分子不需要出现在犯罪现场。

不幸的是，对于俄罗斯网络犯罪分子来说，目前的状况都很有利：被起诉的风险很低，而潜在的回报却很高。其结果是，越来越多的犯罪分子参与到这样的犯罪活动中，造成的损失也越来越高，网络犯罪服务的市场也在壮大。

犯罪分子还利用了内部合作机制缺失这一点。例如，卡巴斯基实验室的专家们知道，一些犯罪团伙成员长期居住和工作在俄罗斯的邻国，而邻国公民也会进入俄罗斯领土来实施犯罪活动。

卡巴斯基实验室正在尽一切可能来阻止网络犯罪团伙的活动，并鼓励所有国家的企业和执法机构展开合作。

针对 Carbanak 活动的国际联合调查是由卡巴斯基实验室发起的，这是首次成功的国际合作范例。如果要看到积极的变化，应该有更多这样的案例。

参考资料：什么是卡巴斯基实验室计算机事件调查？

卡巴斯基实验室一家知名的反恶意安全解决方案企业。但是，该公司还提供全面的保护服务，包括计算机事件调查。

一起事件的证据（主要是以数字数据的形式呈现）需要经过收集和记录。当受害人提出报案时，我们要毫无疑问的进行调查和实验。

卡巴斯基实验室计算机事件调查的责任包括：

- 响应 IT 安全事件并提供快速的情况分析；
- 根据既定程序收集数字证据，确定 IT 安全事件的情况；
- 分析收集到的证据，网上寻找相关的事件信息并进行修复；
- 准备受害人报案所需的资料；
- 为侦查行动提供专家支持。

在响应 IT 安全事件和支持调查行动的过程中，需要处理大量的数据。通过数据分析和恶意对象统计，能够识别网络空间中的犯罪行为趋势。

卡巴斯基实验室的计算机事件调查部成立于 2011 年，由 6 名取证专家组成。