上接B02

克里斯·迈克康其是普华永道网络安全团队的榜样人物。31岁的他头发梳得整整齐齐,胡子剃得干干净净,衣着挺括,一点不像传说中穿着松垮套头衫的“极客”。他成长于北爱尔兰一个农庄,小学时就着迷于电脑,13岁买了一台。他做的第一件事让父母多少有些不安——把它大卸八块。好在他最终搞清楚了如何把所有部件装好。不到一年时间,迈克康其学会了分析电脑病毒和恶意软件。到离开学校的时候,迈克康其已经成立了自己的软件公司。

“我一直喜欢了解万事万物的运行原理,喜欢把它们分解成一点一滴,不管面对的是机器还是其他东西,就是想弄明白。”他带着柔和的爱尔兰口音说。“16年来,我把这当成一个爱好,也当成一份工作。我就是想弄明白那些坏家伙能走到哪一步,该如何对付他们。”

后来迈克康其成了普华永道贝尔法斯特分公司首位计算机鉴证技术人员,现在他负责着以伦敦总部为根据地的网络应对团队。他的手下不是普华永道常会招聘的大学生,有些人确实上过大学,有些人则没有。他们也从英国情报机构收到过简历。有些人会说好几种语言。但对多数人来说,只有一种语言最重要:计算机编码。所有成员都使用社交媒体,对他们来说,网络就像空气一样。

最新成员克里斯·多曼今年二月才加入普华永道,迈克康其在Twitter和LinkedIn上花了数天时间“骚扰”他。“一个星期六早上,我设法拉他到克拉彭去喝咖啡。”他说,然后直接请那个27岁小伙子去普华永道面试。

迈克康其之所以这么殷勤地招揽剑桥大学计算机科学毕业生多曼,显然是因为他在美国国防部举行的“数字取证挑战赛”(Digital Forensics Challenge)取得了骄人成绩。这是一个全球性比赛,参加者都是想成为网络调查者的人,在比赛中他们必须解决摸拟的网络入侵。在来自全球的2000名参赛者中,多曼一路领先,仅屈居于美国国防承包商诺斯洛普格拉曼公司的四人团队之后。

有了这样的实力,彬彬有礼、言语平和的多曼自然不会缺少工作机会,向他发出热情邀请的包括一个反病毒软件公司、几家有名的信息科技安全公司,还有“四大”中的另外一家。

普华永道给多曼这样高级分析员的起薪超过4万英镑,但它能赢得多曼,还有其他原因。用多曼的话说,分析威胁、追踪那些坏家伙,不是在什么地方都能做这样的事。“我在其他地方遇到的人会把这个作为一份朝九晚五的工作来做,但在工作之余,他们不会仍有热情接着做这样的事,他们不想一直阅读这样的东西。”

迈克康其想要的也正是这种投入的热情,他要找的是把网络调查当作爱好的人。“他们并未想到这对他们来说是一种职业,他们会因为高效地做了自己喜欢的事情收到报酬。”

当然,不是所有人都这样想。当迈克康其和他的团队成员找到普华永道时,拥有类似技术的少男少女正成为新一代政府雇佣的黑客或者犯罪集团成员,或者就坐在自己卧室里,高兴时就随手对一个企业作出伤害。

要想理解这林林总总的各类演员在一场网络攻击中扮演了什么角色,可不是一件轻松活。对于普华永道的数字侦探来说,看似随意的字母和数字组合就像犯罪现场留下的脚印一样富有揭示性。这样的序列可能是邮件、银行账号,甚至可能是远在数千英里外的遥控武器。

高持续性威胁(简称APT)——亦即那种顽固的、实力强大的威胁,它们背后往往有政府的支持——是最让客户害怕的。而眼下,显示在普华永道会议室墙上的,就是一个APT,对方的活儿干得很漂亮。

种种迹象显示,越来越多的网络攻击含有政治因素。“作战空间不再只存在于一个国家和另外一个国家之间。”蔡解释说。他来自韩国,擅长研究地缘政治。“你会发现,有国家和政府卷入跟非政府机构的斗争中。”

私营机构意识到了这样的威胁。全球最大法律公司之一Clifford Chance发现,过去一年里,针对该公司的、有政府资助的网络攻击急剧增加。“一直以来都有大量黑客攻击,大部分水平不高。”该公司首席信息官保罗·格林伍德说。“对我们来说,新鲜的是这些攻击背后政府支持的幅度之大,之前我们从未见过这种状况。”他举例说,之前有一个能源公司要卖出,Clifford Chance负责做咨询。有个网络攻击企图监控所有交易方。“调查证明,这个不成功的网络间谍行动的源头是政府,但这个交易本身纯粹是商业性的。”

这种行为已经威胁到一些原本平稳的外交关系。斯诺登泄露的文件揭示美国大量窃听欧洲领导人电话,闹得沸沸扬扬,但文件中同时有大量证据表明,美国针对其他盟国进行了广泛的商业监听活动。美国和加拿大都涉嫌由政府出面支持针对巴西一大公司的商业监听行为。巴西要求美国回答,为什么它的国有石油公司Petrobras被美国国家安全局监听,后者还把信息跟北美的邻国加拿大分享,尽管有公开的誓言要求国防部不应使用任何手段——包括网络——从事任何经济监听行为,因为这会破坏美国的政策。最近几周,类似的争论也蔓延到了欧洲。“美国人在商业和工业层面上都在监听我们,反过来我们也监听他们,因为保卫我们的企业关系到国家利益。”法国前国家情报局主席贝尔纳尔·斯夸西尼10月份接受《费加罗报》采访时说。“没人是傻子。”

如何使用这些信息引起了争论——在某些情况下商业利益可以辩称是国家利益,反过来也一样。由国家控制的实体,不管是主权财富基金,还是冠军企业,都越来越多地被各国用来扩展它们的影响力。“国家安全和商业安全之间的界限是模糊的。”尼克·迈克布拉德说,他曾经担任美国弗吉尼亚州东区联邦检察官,负责针对斯诺登的刑事诉讼。

这一切意味着过去只在政府资助的网络战中出现的技术现在开始被用来针对企业目标。工业间谍活动不断进化,从企图获得商业机密和知识产权转向通过黑客行为实际控制资产。

至今为止,在现实世界中产生最大影响的案例是Stuxnet,2010年这个病毒摧毁了伊朗10%的核生产能力。虽然没有政府正式宣布对此事负责,但媒体一直宣称是美国和以色列干的,而这两个国家也未否认这种猜测。

在Stuxnet出现后大约两年,一个名叫Shamoon(阿拉伯语版的Simon,网络侦探倾向于认为这是病毒作者的名字)的病毒攻击了沙特国有石油公司Aramco(世界最大石油生产商)的计算机系统,把30000个硬盘上的数据删除。沙特官员后来表示,这场攻击显然意在影响公司的生产。

同一个病毒还攻击了卡塔尔的Ras Gas公司,该公司规模很大,主要生产液化天然气。虽然有一个名为“正义之剑”(Cutting Sword of Justice)的黑客组织浮出水面,宣称为此事负责,说这是为了报复发生在叙利亚和巴林的“残酷事件”。分析人士却认为,沙特阿拉伯和卡塔尔都是伊朗眼中的美国代理人。攻击发生在Aramco遭攻击的同一个月,在那不久之前,沙特阿拉伯曾经说它将增加石油生产,以应对任何因制裁伊朗产生的石油供应问题。“政治和经济问题就这样搅到了一起。”蔡说,“Aramco事件是一个经典案例。”

今年夏天,欧洲刑警组织捣毁了一个贩毒集团,它曾经入侵比利时安特卫普港的控制系统,以期控制集装箱,便于运载他们的毒品、武器和现金。安特卫普案还有一点引人注意,根据欧洲刑警组织的说法,这个贩毒集团把此次骗局的技术部分外包给了黑客。

具备发起或者狙击网络进攻的必要技能的青少年供应有限,但是他们所拥有的市场,不管是否合法,都在扩张中。经济衰退可能也扩大了所谓“黑帽黑客”——也就是邪恶黑客——的队伍,因为年轻人的合法就业市场大幅萎缩。

在美国和英国,市场对人才短缺作出了自己的回答。美国网络公司Semper Secure调查发现,在网络安全行业,哪怕你只有一年信息技术行业经验、仅有副学士学位(学的是两年制专科课程),也能拿到91000美元的年薪。根据美国大学与雇主协会的数据,这比美国大学生全国平均年薪(2012年为44455美元)多一倍多。

如果连普华永道这样的大玩家都不得不向不那么资优的候选人敞开怀抱,那么暗黑势力一方必然会开出更好的条件,更会招揽人。犯罪集团通常在封闭式的在线论坛招聘,在那些虚拟市场中,一切都待价而沽——不管是恶意程序,还是要攻击的机器的资料。在这里有意向的黑客可以接受考验,展示他们的技术,就像普华永道的多曼入职时要接受的测试一样,只是版本更加“黑暗”。

在分析中,普华永道发现,网络攻击会出现在预测的时间框架内。在年终即将到来之际,这一类袭击频率增加,因为这个时候,连黑客都会试图“建功立业”,以便给上司留下深刻印象,争取到更多年终奖。BAE Detica的分析师加菲尔德指着一张图表,解释“白帽黑客”和“黑帽黑客”在勤奋工作方面是多么相似。梳理了来自亚洲某国的网络攻击活动后,加菲尔德发现攻击高峰期通常是早上9点到晚上5点之间,午休时会稍稍回落。另外一个高峰期是该国的深夜,亦即美国东海岸的工作时间。加菲尔德由此认为,这些团队采取了轮班工作制度。

普华永道的凯利说,这样井然有序的黑客策略——24小时连轴转,不屈不挠——让大部分企业望而生畏。“他们的技术不见得多么高超,但问题在于坚持不懈。”他说,“你每天朝九晚五地上班,领着工资干着这事,终有一天你会伤及目标。不是因为你手段高超,而是因为你整天做这件事,每天都在做。”

对于凯利的客户来说,幸运的是他也一样坚韧不拔。他向来喜欢把事情条分缕析,看它们是怎样进展的,现在他为世界的安全做这件事。作为全球最精英的企业网络防卫团队成员之一,他每天与那些看不见的敌人过招,磨炼技巧。在虚拟世界,这差不多就是一对一的肉搏战。

“网络空间最可怕之处在于它是完全不对称的。”他说,“可能只需要一个人就能把整个系统关掉。如果那个人有能力关掉许多系统,那就会危及到整个国家,甚至是整个世界。所以,构建防御体系时,我心里就一直敲着这样的警钟。”

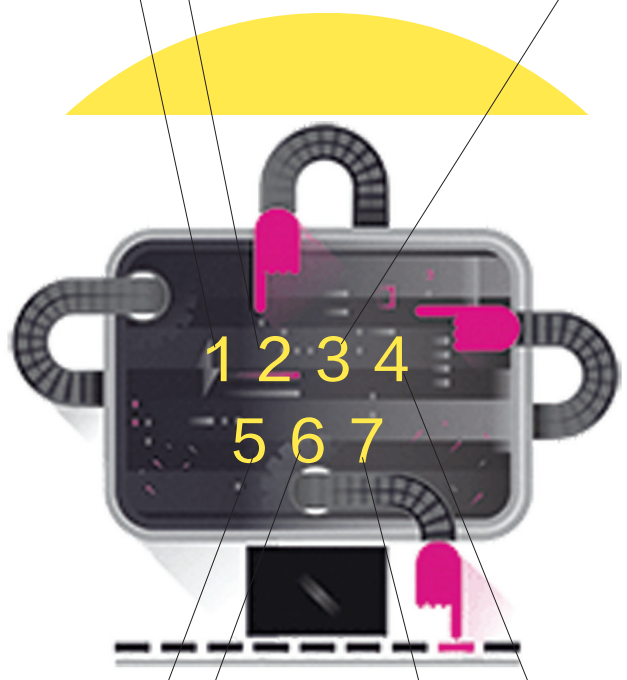
南都供稿

原作:Caroline Binham 原载:FT Magazine

网址:http://www.ft.com/cms/s/2/bccc8f3c-523c-11e3-8c42-00144feabdc0.html#ixzz2liCluXQm

编译:Dawn

网络攻击过程简析



1 踩点
黑客对于目标公司进行研究,董事会成员、管理层、所在地点、供应链都是研究对象。

2 武器“研发”
黑客在特意设计的文件(比如某个行业大会的PDF文件)内嵌入恶意软件,以便诱使目标公司的员工打开它。

3 传播
恶意程序通过预订邮件被感染的U盘或其他移动设备等进入目标,旨在攻击对方的系统。

4 寻找机会
病毒试着找到系统的弱点,以便释放代码。

5 安装
如果成功打入敌人内部,恶意程序会自行在电脑内安装,找到进入系统的入口。

6 指挥与控制
恶意程序向黑客的指挥与控制中心发出信号,要求它发出指令。

7 完成任务
数据被盗走或摧毁,黑客的目标达到。