NSA局长、美国网军司令迈克尔·罗杰斯

数字军备竞赛

美国国安局正在准备网络战

美国国家安全局(NSA)的大规模监听只是"冰山一角"。爱德华·斯诺登最新披露的文件显示,美国国安局正在为未来的数字战争做准备,一场控制互联网的斗争已经有条不紊地展开。

现代快报记者 潘文军 编译

已经实行8年的实习生招聘计划

一般情况下,一个实习申请者如果想要参加社会项目,成为志愿者,他需要一份耀眼的简历。但是"Politerain"计划需要的是能够"打破常规"的实习生。

"Politerain"不是普通的公司项目,它是美国政府情报机构国家安全局运行的一个项目。更确切地说,它是由NSA麾下的"获取特定情报行动办公室"(TAO)负责的一个项目。而TAO部门的职责就是侵入别人电脑。

实习生们被告知:对第三方电脑的"研究"包括通过攻击硬件远程破坏对手电脑、路由器和网络设备。例如,他们可以使用一个叫做"Passionatepolka"的程序来远程围堵对方电脑的网卡;"Berserkr"程序可以在对方电脑里植入木马程序;另一个名为"Bamfire"的程序则可以清除对方电脑里的BIOS系统数据。

实习生的任务可能还包括远程销毁对方电脑的硬盘驱动器。实习的最终目的是让实习生学会"像攻击者一样思考"。

NSA以此为标准招聘实习生已经有8年时间,"攻击者心态"已经成了NSA网络间谍的清规铁律。事实上,美国及其"五眼联盟"(美国、英国、加拿大、澳大利亚和新西兰)盟友已不再满足于大规模监听活动所得到的情报,他们想要的更多。

"D武器"的诞生

根据斯诺登提供的文件,Politerain计划的目的是使计算机网络系统瘫痪以便于进行远程控制,覆盖面包括能源供给、水利系统、工厂、机场和金融系统。

20世纪,科学家们发明了所谓的"ABC武器"——原子(atomic)武器、生物(biological)武器和化学(chemical)武器。人们花了几十年来部署和调节这些武器。现在,新的"D武器"——数字(digital)武器将战争带入互联网时代,几乎没有任何国际公约或者监管机构可以监控这些"D武器"的使用,所以,优胜劣汰是"D武器"的唯一法则。

加拿大媒体理论家马歇尔·麦克卢汉几十年前就预见到了事情的发展。1970年,他曾经写道:"第三次世界大战是游击信息战,军用和民用之间没有区别。"这是对今天的间谍们的真实写照。

美国早在上世纪90年代就提出了网络战概念,近年来更是大力发展网络部队,打着维护国家利益的旗号在网络空间积极扩军备战。

美国的陆海空军和海军陆战队都建立了自己的网络部队,但是网军的官方领导机构是NSA。这并非巧合,NSA局长迈克尔·罗杰斯上将还兼着美国网军司令的职务。据悉,罗杰斯帐下有接近40000名雇员,负责在网上搜罗情报和进行网络攻击。

美国网军由3个分支组成,除保护美国国内电网、核电站等重要基础设施的网络部队外,还有协助海外部队策划并执行网络袭击的"进攻性"部队,以及保护国防部内部网络的"防卫性"部队。前者已于2013年9月投入运行,后两个分支也将在今年组建完成。

大规模监控只是网络战争的前提

从军事角度看,在美国准备网络战争的策略中,监控互联网只能算是"0阶段",也就是预备阶段。NSA的内部文件表明,监控互联网是其他一切行动的前提,监控的目的是检测敌方系统的漏洞。网络战的第一个阶段是将一些程序"隐形植入"到敌方的系统中,第二个阶段是让敌方的电脑变成可以"永久访问"的电脑,然后才进入到数字战争的第三阶段——"控制"敌方的电脑。到达这个阶段,美国军方就可以控制或摧毁敌方的电脑系统以及网络。一旦如此,敌方的重要基础设施,包括保持社会运转的重要能源、通讯和运输都将瘫痪。内部文件指出,美国的最终目标是"实施控制的升级"。

斯诺登

NSA曾在一份声明里说:"未来主要的冲突会在网络空间中展开。"为了应对这个情况,美国政府正在付出巨大的努力,用数字化武器武装自己的网络部队。在2013年情报机构的秘密预算中,预计NSA大约需要10亿美元来提高计算机网络攻击的实力,预算中还包括一项3200万美元的"非常规解决方案"项目。

近年来,美国和它的"五眼联盟"盟友已经开始使用恶意软件攻击敌对国的电脑设备和网络设施。这些恶意软件包括攻击伊朗核计划的"震网"病毒,感染了德国总理默克尔身边高级工作人员U盘的间谍木马程序"regin"。"regin"还在2011年攻击了欧盟委员会、欧盟行政部门和比利时电信公司Belgacom。2010年,美国还在韩国和其他盟友的帮助下,"直接侵入了朝鲜网络",并植入恶意软件,从而成功监控朝鲜网络的内部运作。

由于网络间谍可以突破几乎所有常规安全软件,所以几乎全球所有互联网用户都存在受到网络攻击的风险。

斯诺登最新披露的文件还提到了一些新动向。一种名叫Quantuminsert的攻击软件已经被媒体广为报道,但其实它的成功率非常低,已经被诸如Quantumdirk之类更可靠的攻击软件所取代了,后者可以被植入"脸谱"或雅虎聊天工具中。而那些感染了Straitbizarre病毒的电脑则变成了"即用即抛"的"攻击手"。这些"攻击手"可以从NSA的量子网络接受信息,根据所收邮件的命令进行大规模的攻击活动,完成攻击后即被弃用。秘密特工还能够利用手机Safari浏览器中的一个漏洞远程植入恶意代码,获取敏感数据。

斯诺登提供的文件显示,在网络战争之中,很难区分士兵和平民,任何互联网用户都可能遭遇攻击,而且,网络战争一样可以在线下世界制造危险。举例来说,如果一家医院的电脑系统受到"Bamfire"程序攻击,那么病人的治疗就会受到影响,哪怕这些病人从来没用过手机。

对于在网络世界的行动,情报机构都采取了"合力推诿"的策略。为了不留痕迹,他们都努力让人无法查到攻击者的踪迹。

网络间谍正在以惊人的方式破坏着世界各地的法制根基。互联网正在成为超级大国情报机构之间角力的一个无法无天的领域。

要想对网络行为追责十分困难,需要大量的取证工作来确认每一个行为究竟是谁做的。斯诺登提供的新文件中提出了几个点子。比如可以使用"全键盘"键盘记录器秘密截取受害人敲击键盘的所有记录,以备日后检查。

NSA的黑客部门

为远程操作中心(ROC)工作的雇员有个代号叫S321,该机构总部设在马里兰州米德堡,是NSA负责秘密行动的最关键的团队。S321的员工在NSA一栋主要大楼的3楼。在斯诺登提供的文件中,有一名NSA员工的回忆。他说:"ROC的人就是一小撮黑客。"最初,S321雇员以一种更特别的方式工作,但是现在他们的工作流程更系统化。2005年夏季,在NSA大幅度扩大ROC规模之前,该部门的座右铭是"你的数据就是我们的数据,你的设备就是我们的设备。"

特工们坐在电脑前,全天候轮班工作。究竟NSA离"占据全球网络主导地位"的目标有多近,则需要代号为"违法"的S31177部门来说明。

该部门的主要任务是跟踪国外网络攻击,进行观察和分析,然后选择最佳时机抽走敌方情报机构的信息。这种"网络反情报"形式是现代间谍活动中最精妙的算计。

美国也曾遭他国网军攻击

斯诺登提供的文件不仅曝光了美国的网络攻击力量,也曝光了其他国家的网军实力。"违法"部门这些年来一直在吸取世界各国网络部队的经验,并且编辑了其他国家通过恶意软件进行网络攻击的数据库。

斯诺登提供的文件显示,近年来,NSA和美国"五眼联盟"的盟友对其他国家的网络发动过多次攻击。2009年的一份文件指出,"违法"部门的职责是"探索、了解和评价"外来攻击。而另一份文件上写着:"偷他们的工具、谍报、目标和利益"。

斯诺登提供的文件还提到了NSA几年前做的内部损害评估。评估报告指出:美国国防部记录在册的就有超过30000起事故;超过1600台链接互联网的电脑遭遇黑客攻击。这些事件造成的损失和维修费用超过1亿美元。

被黑客攻击命中的"敏感军事技术"包括空中加油计划、军事物流规划体系、海军导弹导航系统、核潜艇信息、导弹防御系统以及其他一些绝密国防项目的信息。

想要"知道一切"的当然不止美英俄等几个大国。几年前,美国特工发现了源于伊朗的偷窥监控操作;他们还发现过源于法国的网络攻击行为,那次攻击被命名为"Snowglobe"。

利用"僵尸军团"展开反击

NSA和"五眼联盟"的盟友早就在通过自动化手段搜寻国外网络攻击的黑客。监护系统能够识别入侵程序,确保黑客没有达到目标。

斯诺登提供的文件中提到了相对原始的低轨道离子加农炮(LOIC)。这个名词指的是黑客组织"匿名者"攻击网站时使用的恶意软件。遇到这种攻击时,Tutelage防护软件能够识别黑客IP,并阻止来自该IP的攻击。

NSA也能够转防御为进攻。这种方式被描述为"反向工程师,重新规划软件",还涉及僵尸网络,有时会牵扯到数以百万计的被偷偷安装了软件的普通互联网用户的电脑。这些电脑因此可以成为远程"僵尸军团"让公司瘫痪,进而敲诈勒索。如果受感染的主机在美国,相关信息就会被提交给联邦调查局(FBI)的受害者援助办公室。然而,受到感染的僵尸主机可以被"Quantumbot攻击程序"劫持,被重新定向到NSA那里。在NSA的文件里,这个项目被称作"挑衅勇士",据说可以提供"无处不在的网络分析瞭望点"和"被抛弃的非归属电脑网络攻击(CNA)节点"。该项目使人们的电脑变得脆弱,而且能够偷偷摸摸地使用无辜受害者的电脑。Quantumbot攻击程序不仅不为私人互联网用户提供保护,反而利用他们作为"人体盾牌",掩饰自己的攻击行为。

NSA远程操作中心(ROC)的专家们拥有一整套数字万能钥匙和撬棍,可以访问受到最严密保护的电脑网络。他们给自己的工具起了个很有攻击性的名字——"锤头商人",仿佛他们在经营一家专门面向网络罪犯的应用程序商店。"锤头商人"是一个植入性软件,可以对互联网电话进行录音。"狐狸酸"软件则可以不断增加已经安装在目标电脑上的恶意程序的功能,该项目的标志是一只狐狸的尖叫声。NSA拒绝对操作细节进行评论,并且坚持认为,自己没有触犯法律。

既是警察,又是强盗

随着网络战武器的发展,当涉及到闯入并刺探第三方网络时,一个悖论出现了:如何才能让情报机构确认自己不会成为自己正在实施的侵入行为的受害者?黑客、罪犯或其他情报机构难道不会用同样的方法对付自己?

为了控制恶意软件,远程操作中心通过自己的影子网络与这些软件保持联系,一般是通过高度敏感的电话录音、恶意程序和密码传送进行联系。

侵入网络的诱惑是巨大的。搜集到的任何VPN密钥、密码和后门都有非常高的价值。那些拥有密码和密钥的人,理论上可以抢劫银行账户、阻止军事部署、克隆战斗机甚至关停电厂。这一点也不比"拥有全球网络主导地位"的意义小。

但情报机构的世界是个"精神分裂"的世界。NSA的任务是保卫互联网的安全,但同时他们又要"开发"互联网的安全漏洞。它既是警察又是强盗,坚持着间谍世界无处不在的座右铭:"掏出别人的秘密,保护好我们自己的秘密。"

作为结果,一些被黑的服务器就像上下班高峰期的公交车,人们不断进进出出。不同的是,服务器的主人根本不知道谁在里面。而那些想当然的权威机构却袖手旁观。

不知情的"数据骡子"

这听起来有些荒谬:间谍们一边忙着监视别人,一边却被其他间谍监视着。对此,间谍们经常试图掩盖他们的踪迹,或者制造假的网络轨迹。在技术上,远程操作中心(ROC)制定了假的网络轨迹:在第三方电脑被侵入后,开启收集数据的程序。但是收集到的数据不会直接传输到ROC的IP地址。相反,这些数据会被输入到一个"替罪羊"那里。这意味着窃取来的信息最终可能会出现在别人的服务器上,使得他们看上去像是肇事者。

之前的数据最终都被传输到"替罪羊"那里,当然NSA在传输过程中会截获数据拷贝,并将截获的数据拷贝发送到ROC那里。但是,这种掩盖手法增加了控制风险,或者说是有关机构不受控制的风险。

可以被系统侵入、监视和用作"僵尸网络"的当然不只是电脑,手机也可以被用来窃取主人的信息。不知情的受害者其手机已经感染了间谍程序,会将办公室的信息收集到手机上;受害人下班后回到家,这些信息就会被远程获取。网络间谍甚至会用贩毒俚语称呼这些不知情的帮凶——"不知情的数据骡子"。

无法无天的网络世界

NSA的特工不用担心被抓。部分原因是他们在一个强大的机构工作,另一部分原因则是因为他们的所作所为不会留下任何可以在法庭上被呈堂的证据。如果没有犯罪证据,就不能进行法律的惩罚,情报机构并不受议会控制,也没有国际协议。迄今为止,几乎没人因为使用这种新型的"D武器"而遭遇风险,这是一个几乎不存在政府监管的领域。

爱德华·斯诺登透露,NSA领导下的世界各地情报机构正竭尽全力利用互联网领域的法律真空。在最近一次接受美国公共广播的采访时,斯诺登表示了自己的担忧:"攻击总是优先于防御。"

斯诺登说:"我们需要做的,是建立互联网世界的国际行为准则。"

NSA在米德堡的司令部