Stuxnet病毒 开启网络战争新形态

2008年,伊朗总统马哈茂德·艾哈迈迪-内贾德视察纳坦兹铀浓缩设备,后来该核设施成为Stuxnet病毒的攻击目标

以色列的情报机构摩萨德用一种高科技的电脑病毒Stuxnet蠕虫病毒袭击了伊朗的核设施,作为首个具有地缘政治意义的数字化武器,Stuxnet蠕虫病毒将改变战争开展的形式,今后将会涌现出更多的网络战争武器。

摩萨德前负责人梅尔·达甘

2004年卫星图片上的伊朗纳坦兹核设施

“数字克星”扩充武器种类

在从以色列特拉维夫市到海法市的高速公路交叉道附近一座山上,有一处建筑群,占地面积有好几个足球场那么大,用高墙和铁丝网封闭了起来,这就是以色列情报机构总部摩萨德(全称以色列情报和特殊使命局)。摩萨德好似以色列的一处“现代堡垒”,严禁新闻界和政界等人士进入。

但在2011年1月6日,摩萨德严禁访客的政策暂时放宽,一辆窗户暗黑的小面包车停在了摩萨德附近一家影院的停车场里。面包车里的记者们被要求交出他们的手机和录音设备,时任摩萨德负责人梅尔·达甘邀请他们前往摩萨德总部,那一天也是达甘担任摩萨德负责人的最后一天。记者们来到摩萨德总部,采访、记录摩萨德对伊朗核设施展开的网络袭击。

达甘表示,如果对伊朗展开军事袭击或将带来风险,而且军事袭击无法阻止伊朗核计划,只能暂时减缓其进度。因此,达甘更青睐不进行常规战争就能阻碍伊朗核计划的方式。一种新的神奇武器应运而生,它就是Stuxnet蠕虫病毒。

Stuxnet蠕虫病毒能入侵未连接互联网的高度保密的计算机,这在以前几乎被认为是无法实现的。2010年6月,Stuxnet蠕虫病毒袭击了伊朗纳坦兹核设施的计算机,纳坦兹核设施是科学家们制作浓缩铀的地点,此次袭击击中了伊朗核计划的核心。

Stuxnet蠕虫病毒是世界上首个具有地缘政治意义的网络武器,著名德国黑客组织“混乱计算机俱乐部”的弗兰克·列格尔将之称为“数字克星”。Stuxnet蠕虫病毒的诞生意味着现代武器种类的扩充,使得利用计算机程序实施军事袭击成为可能。

Stuxnet蠕虫病毒袭击伊朗核设施一年后,世界上没有一个网络安全公司或主要国家的政府不知道Stuxnet的名字,为了让人们进一步了解Stuxnet蠕虫病毒和它背后的故事,德国《明镜》周刊记者前往以色列进行了采访。

利用西门子系统的安全漏洞

美国Symantec计算机安全公司以色列分公司负责人萨姆·安吉尔说:“Stuxnet蠕虫病毒是我们见过的最为复杂的病毒攻击,这种针对成熟的、独立的工业系统进行的袭击非比寻常。”受到Stuxnet蠕虫病毒袭击的国家包括伊朗、印度尼西亚、马来西亚和白俄罗斯,白俄罗斯一个叫做谢尔盖·尤拉森的人发现了Stuxnet蠕虫病毒。

据分析,Stuxnet蠕虫病毒在全球范围内已感染了约10万台电脑,包括伊朗的6万多台,印尼的1万多台和印度的5000多台。发明者们对Stuxnet病毒进行了编程,使得病毒在入侵后,首先能告诉两台控制和命令服务器被感染的电脑是否使用Step7系统,Step7系统是德国西门子公司研制的工业控制系统,伊朗纳坦兹核设施的离心机使用的就是Step 7系统。

Stuxnet病毒利用了Windows系统中的安全漏洞,从而操纵计算机系统。由于Windows系统中的安全漏洞,Stuxnet病毒能通过U盘进入系统。一旦U盘连接电脑,就开始在暗中安装病毒。

Stuxnet病毒会首先搜索防病毒程序,然后设法避开它,如果无法避开则取消自行安装。第二步中,Stuxnet病毒会寄生在操作系统中管理U盘的部分,在那里建立校验和(用于校验目的的一组数据项的和),当校验和的数值达到19790509时,病毒就停止感染。建立校验和的真实用途目前还未被破解,这可能是某种编码。19790509可以代表1979年5月9日,伊朗伊斯兰革命后,著名犹太商人哈必卜·埃勒加尼安在伊朗德黑兰被处死的那天。这是一个巧合?一种挑衅?还是故意用来转移注意力的东西?

Stuxnet病毒如何进入纳坦兹核设施也是个谜。Windows操作系统中存在一些不为人知的安全漏洞,寻找这些漏洞既是黑客们的挑战也是一种商业模式。在黑市上,一个未知安全漏洞可以卖到10万美元以上的价格,而Stuxnet病毒利用的未知安全漏洞至少有4个。

美国协助?以色列自主研发?

Symantec以色列分公司经理安吉尔认为,不对西门子系统非常了解的话,是无法编写出Stuxnet蠕虫病毒的。“西门子系统未知安全漏洞交易的黑市并不存在,”安吉尔说,“西门子系统的使用不够广泛。”但摩萨德是如何得到纳坦兹核设施使用西门子系统的相关技术信息的呢?

很多人猜测,美国帮助摩萨德研制了Stuxnet蠕虫病毒,美国爱达荷州的一个政府研究机构专门研究伊朗所使用的西门子控制技术,Stuxnet病毒的基础研究可能就是在那儿完成的。在那之后,Stuxnet病毒可能在内盖夫沙漠迪莫纳附近的以色列核研究中心进行了检测。

但熟悉Stuxnet病毒袭击的以色列消息人士坚称,Stuxnet病毒完全是以色列本国的产物。他们认为,以色列军事情报机构的精锐部门编写了部分代码,然后由摩萨德完成了剩余部分,Stuxnet病毒显然也是由摩萨德带入纳坦兹核设施的。该消息来源还表示,摩萨德试图在黑市上购买一台纳坦兹核设施使用的那种离心机,但没有成功,最后在情报部门的帮助下,一个以色列武器制造商制作出了纳坦兹核设施离心机的模型,用于检测Stuxnet病毒。

2009年夏天时以色列已经准备好了病毒袭击,Stuxnet病毒在2009年6月22日下午4点31分被启动。袭击瞄准了5个伊朗机构,并发动了3波攻击。后两次袭击分别发生在2010年3月和4月。

一家欧洲情报机构得出的分析称,一个程序员编写Stuxnet蠕虫病毒需至少耗时3年。Symantec计算机安全公司估计,在模型设施中的检测就需要5-10名程序员花费半年时间完成。德国联邦安全委员会认为,Stuxnet蠕虫病毒的研发“不可能是非政府行为”,决定建立一个全国性的网络安全防御中心。Stuxnet蠕虫病毒从根本上改变了人们对数字攻击的看法,美国政府最近发布了新的网络战争原则,将网络袭击定义为战争行为。

可媲美密码机的巨大成功

摩萨德将Stuxnet蠕虫病毒视为巨大的成功,可以跟二战中的恩尼格玛密码机相媲美。但以色列军方却没这么乐观,以色列军方认为Stuxnet蠕虫病毒被发现会让以色列付出很大代价。

一台伊朗IR-1型离心机的转速为1064赫兹,当离心机第一次被病毒感染出错时,会持续以1410赫兹的转速运转15分钟,然后回到正常转速。27天以后Stuxnet蠕虫病毒再次发起攻击,这次让离心机以低于正常转速几百赫兹的速度运转了50分钟。离心机出错产生的过度离心力让铝管扩大,提高了离心机部件相互冲撞的危险,最终可能导致离心机的摧毁。

6组各含有164个离心机的机组都报告产生了以上故障,伊朗核计划当局认为Stuxnet蠕虫病毒破坏了约1000台离心机。伊朗承认自己的核计划遭到了阻碍,称核计划遭受了“潜在的重大损失”。

摩萨德前负责人达甘没有发动战争而实现了自己破坏伊朗核计划的目标,但伊朗还有8000台离心机,并且第二代的IR-2型离心机可以在高达1400赫兹的转速下顺利运转,Stuxnet病毒将不会对它们造成威胁。也许摩萨德很快需要研发新版本的病毒,用于下一轮秘密网络袭击。

两名间接为以色列情报机构工作的年轻人表示,他们的目标是网络袭击而非防御。他们是一个国际黑客精英组织的成员,有传言称这两人参与了摩萨德研发Stuxnet蠕虫病毒的一些基础工作。其中一名黑客称:“除了在电影里,人们之前从未见过像Stuxnet蠕虫病毒这样的东西。”

Symantec计算机安全公司已发现了Stuxnet蠕虫病毒的另一种版本,含有更为复杂的编码,但还未被激活使用。Symantec计算机安全公司的员工称:“Stuxnet蠕虫病毒是我们希望永远不会再见到的东西。”但这种愿望已基本上不可能实现。

快报记者 李欣 编译