拖延伊朗核计划“震网”攻击细节首披露

荷兰间谍几次潜入实施攻击

多年来，针对伊朗核计划的“震网”病毒攻击一直是个谜：美国和以色列是如何将他们的恶意软件植入伊朗高度安全的铀浓缩工厂的电脑系统的？

美国媒体日前根据荷兰的一份报告首次披露，荷兰情报机构在美国中央情报局和以色列情报机构摩萨德的要求下，招募了一名内奸，潜入伊朗核设施，利用美国开发的“震网”蠕虫病毒，实施了攻击。“震网”是一种旨在破坏伊朗核计划的新型病毒，它实际上开启了网络战争时代。

积累情报

这次著名的秘密行动被称为“奥林匹克行动”，由美国和以色列主导，参与方包括美国国家安全局、美国中央情报局(CIA)、摩萨德、以色列国防部和以色列国家情报总局。据消息人士透露，荷兰、德国和法国也参与了进来，英国情报部门据信也发挥了作用。行动的目的不是彻底摧毁伊朗的核计划，而是将其推迟一段时间，为制裁和外交手段的生效争取时间。最终，这一战略成功地帮助伊朗回到谈判桌前。

据报道，伊朗的核计划多年来一直被搁置，但在1996年进入了高潮，当时伊朗从巴基斯坦科学家阿卜杜勒·卡迪尔·汗那里秘密购买了一套蓝图和离心机部件。2000年，伊朗在纳坦兹破土动工，计划建造一座可容纳5万台离心机的设施。

在此背景下，“奥林匹克行动”实施。实际上，行动开始阶段聚焦于情报搜集，病毒攻击并未被提上日程。据消息人士透露，2000年，荷兰国家安全情报局入侵了伊朗一个重要国防组织的电子邮件系统，以获取更多有关伊朗核计划的信息。在接下来的两年里，以色列和西方情报机构一直在秘密监视纳坦兹核项目的进展。

因为伊朗纳坦兹核工厂的离心机基于卡迪尔·汗从一家荷兰公司获取的设计，荷兰国家安全情报局与美国和英国情报机构一道，渗入了卡迪尔·汗的欧洲顾问和幌子公司的供应网络，提供有关伊朗从欧洲采购设备的活动的关键情报以及有关离心机本身的信息；德国提供了西门子公司生产的工业控制系统的技术规格和知识，这些系统曾在伊朗核工厂用于控制旋转离心机，据信法国也提供了类似情报。

2003年，英国和美国情报部门截获了一艘载有数千台离心机部件的船只，这艘船驶往利比亚，上述部件与纳坦兹使用的离心机型号相同。次年，美国把缴获的部件运到田纳西州橡树岭国家实验室和以色列的一个实验室。在接下来的几个月里，两国科学家组装了这些离心机，并对它们进行了研究，以确定伊朗可能需要多长时间来制造核弹，并由此产生了破坏离心机的阴谋。

秘密暴露

2009年，攻击者决定改变策略并于当年6月、2010年3月和4月分别发布了新版本的代码。这些版本没有关闭离心机上的阀门，而是改变了离心机旋转的速度，或者将离心机加速到设计允许的水平，然后使其减速。其目的是破坏离心机并破坏浓缩过程的效率。

但他们后来的策略有一个缺点——攻击者在这个版本的代码中添加了多种传播机制，以增加它到达纳坦兹内部目标系统的可能性。这导致“震网”病毒失去了控制，先是蔓延到5家承包商的其他客户，然后蔓延到世界各地的数千台其他机器上，导致“震网”病毒在2010年6月被发现并公之于众。

在“震网”病毒被发现几个月后，以色列的一个网站报道，伊朗逮捕了纳坦兹的几名工作人员并可能处决了他们。虽然由于过早被发现，“震网”病毒并没有显著地推迟伊朗的核计划，但它确实为外交和制裁争取了时间，使伊朗回到谈判桌上来。

“震网”病毒还改变了战争的本质，并引发了一场网络军备竞赛，它让一些国家认识到利用网络攻击来达到政治目的的价值。美国中央情报局和美国国家安全局前局长迈克尔·海登上将承认，“震网”超级工厂病毒袭击具有开创性，其意义和广岛、长崎的原子弹袭击相当。

实施袭击

当时，荷兰国家安全情报局已在伊朗招募了一名间谍，在CIA和摩萨德提出要求后，前者帮助这名间谍在伊朗成立了两家幌子公司，希望以此打入纳坦兹。

建立一个有员工、客户和记录显示活动历史的虚拟公司需要时间。2005年底，伊朗宣布退出暂停核试协议。2006年2月，伊朗开始在纳坦兹的一个试验工厂里提炼第一批六氟化铀。2007年2月，伊朗在纳坦兹工厂安装了第一台离心机，正式启动了铀浓缩计划。

与此同时，美方攻击代码的开发工作已经进行了一段时间。2006年，有人用离心机进行了一次破坏试验，并将试验结果提交给了时任美国总统小布什。

到了2007年5月，伊朗在纳坦兹安装了1700台离心机并计划到夏天将这一数字增加一倍。但在2007年夏天之前的某天，荷兰间谍进入了纳坦兹。这名训练有素的间谍伪装成机械师进入纳坦兹，并在此后几个月内多次出入。虽然他的工作并不包括安装离心机，但他探清了收集系统配置信息的位置。“(他)必须……在几次时间内收集到(可用来)更新病毒的必要信息。”一位消息人士说。

消息人士没有提供有关间谍收集到的信息的细节，但“震网”病毒是一种精确攻击工具，只有当它发现设备和网络条件的具体配置时，才会发动破坏。根据内鬼提供的信息，攻击者能够更新代码并提供更准确的精度。

事实上，有证据表明在此期间代码发生了更新。安全公司赛门铁克称，攻击者在2006年5月和2007年2月更新了代码，当时伊朗刚刚开始在纳坦兹安装离心机。但他们在2007年9月24日对代码做了最后修改，修改了发起攻击所需的关键函数，并在那天编译了代码——编译代码是启动代码之前的最后一个阶段。

该代码的设计目的是关闭离心机上的出口阀门，这样气体就会进入离心机但无法排出，如此就能提高离心机内部的压力，并随着时间的推移造成破坏和废气。

“震网”病毒只有一种传播方式——通过U盘。纳坦兹核工厂的西门子控制系统没有连接到互联网，纳坦兹的工程师们用U盘上的代码编写控制系统的程序，所以间谍要么自己直接安装代码，把USB插入控制系统，要么感染了一名工程师的系统，当后者用U盘编写控制系统程序时，他就毫不知情地发送了“震网”病毒。

达成任务后，这名间谍没有再回到纳坦兹，但恶意软件在整个2008年都在进行破坏。

据《广州日报》报道

50余个欧亚国家共商“一带一路”合作发展

新华社西安9月10日电(记者 杨一苗 李华)来自58个国家的政界、商界人士及学者10日齐聚西安，共同参加2019欧亚经济论坛，共商“一带一路”合作与发展。

2019欧亚经济论坛于9月10日至12日在陕西省西安市举办，主题为“共建‘一带一路’：高水平合作，高质量发展”。旨在通过欧亚国家间多领域、多层次对话，推动形成国家层面、国际组织、大型企业、地方政府广泛参与的伙伴关系。

本届论坛设开幕式暨全体大会，以及金融、生态、文旅、气象、科技等10个平行分会。来自上海合作组织成员国、观察员国、对话伙伴国及“一带一路”沿线国家政府首脑及要员，重要国际组织代表；相关国家驻华使节，国内外友好城市代表；国内外商会组织代表；世界500强企业、大型央企、国内外金融机构负责人、专家学者等千余人参会。

欧亚经济论坛发起于2005年，每两年举办一届，已成为中国与欧亚国家共建“一带一路”的重要平台之一，目前已促成能源俱乐部、开元城市发展基金、跨国数字图书馆建设等对外合作意向70多个。

近四分之一德国网民曾遭遇购物欺诈等网络犯罪

新华社柏林9月9日电(毛竞)德国信息技术安全局9日在柏林发布2019年度德国《数字化晴雨表》调查报告表明，德国受访者中24%的网民遭遇过网络犯罪，在线购物是重灾区。

报告显示，2018年德国共发生27.2万起网络犯罪，比2017年增加8%。在网络犯罪受害者中，36%的人在线购物时遭遇过欺诈，28%的受害者个人私密信息曾在互联网上被窃取，26%的人电脑曾遭到病毒软件的攻击，18%的人网络账户被盗。此外，遭到过网络霸凌和勒索软件攻击的受害者比例均为13%。

调查发现，青少年是网络犯罪的主要受害群体。这不仅是因为青少年上网更频繁，也在于其风险防范意识较年长者薄弱。

此次调查由德国信息技术安全局和德国警方于今年4月联合进行，共有2000名年龄在16岁到69岁之间的德国网民参与了调查。