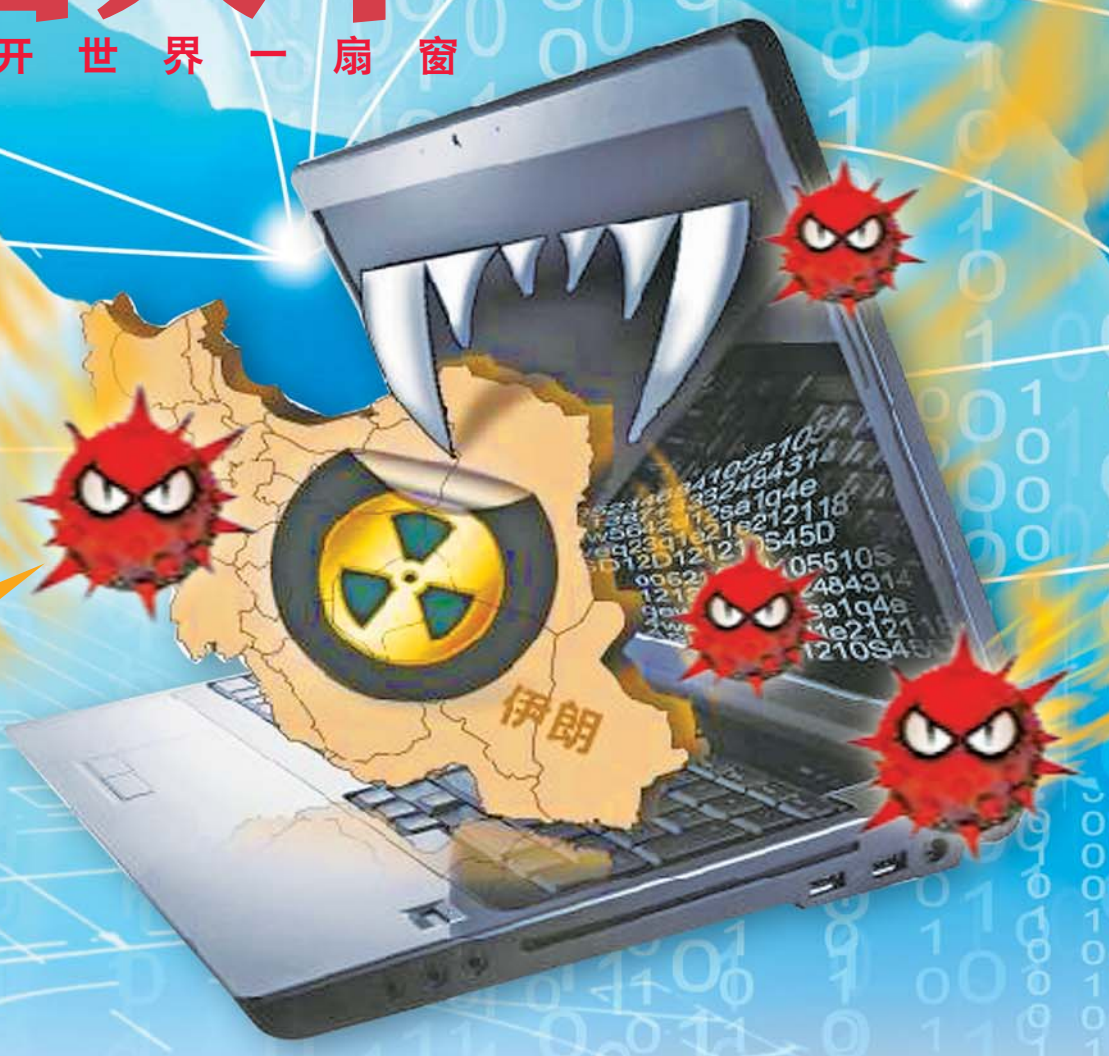

“火焰”病毒

主要功能：

收集情报。

主要特点：

“体型”不算小，约为20MB；

能操控蓝牙设备收集情报；

能记录音频；

采用游戏语言编写，与超人气游戏“愤怒的小鸟”的语言相同。

超级病毒“火焰”点燃网络间谍战

近日，一个名为“火焰”的电脑病毒入侵伊朗等中东国家，收集信息情报，几千台电脑中招。这个病毒被称“超过已知任何一种”电脑病毒。“火焰”究竟从何而来，意欲何为？位于日内瓦的国际电信联盟说，“火焰”是危险的间谍工具。或许，这是又一次针对伊朗的间谍战。

入侵中东 ▶ 几千台电脑中招

伊朗国家计算机紧急情况应对小组5月28日在其协调中心网站上发布声明说，经多月调查，已确认一种名为“火焰”的新型电脑病毒，并且这种病毒可能与伊朗境内部分机构出现的大规模数据丢失事件有关。

卡巴斯基实验室表示，“火焰”病毒已入侵伊朗、以色列、巴勒斯坦、叙利亚、黎巴嫩、沙特和埃及等中东国家和地区的大量电脑，世界范围内受感染电脑数量估计在1000至5000台之间。

主要功能 ▶ 收集情报和数据

据俄罗斯IT安全公司卡巴斯基实验室发言人维塔利·库柳克介绍，这一病毒呈现木马病毒和蠕虫病毒的部分特征，可谓目前结构最复杂的电脑病毒，它具有一些独特之处：

普通电脑病毒往往采用精炼的编程语言，以达到瘦身隐藏目的。而“火焰”病毒是一个庞大的程序包，包含20多个模块，其大小约为20MB。

这种病毒不会中断终端系统，其目的只是收集情报；

除了具备普通电脑病毒的数据窃取手段之外，“火焰”病毒还能记录来自电脑内置话筒的音频数据；

通过蓝牙信号传递指令也是“火焰”病毒罕见的功能。它能启动被感染电脑的蓝牙设备，使它成为攻击周边蓝牙设备的“灯塔”。

库柳克说，“火焰”病毒的设计十分复杂，绝非普通开发者能够独立完成。该病毒的攻击范围很窄，主要针对企业、学校和科研机构。它既没有被用来盗取银行账号，也有别于黑客常用的工具。

病毒利用“视窗”操作系统漏洞侵入，可借助局域网络、打印网络和USB接口等传播。

病毒编写者借助北美、欧洲和亚洲等地区大约80个服务器操控病毒。

强大无比 ▶ 超过已知任何病毒

卡巴斯基实验室技术人员罗埃尔·斯霍文伯格说，“火焰”病毒程序代码量是两年前攻击伊朗核电站的“震网”病毒20倍、普通商业信息盗窃病毒的100倍，包含大约20个程序模块。

卡巴斯基实验室在官方网站的新闻稿中说，以复杂程度和功能效力衡量，新现身的“火焰”病毒“超过已知任何一种”电脑病毒。

但也有不少机构和专家质疑卡巴斯基实验室这种说法。Webroot公司高级管理人员乔·雅罗赫说，这种病毒易被清除，“有不少比它更加危险的病毒”。

间谍工具 ▶ 已自成一支“军队”

“火焰”病毒引起人们对网络间谍活动的关注，伊朗网络安全部门表示“火焰”和著名的“震网(Stuxnet)”、Duqu病毒有“密切关系”。“震网”和Duqu被看做是最早出现的两种“网络间谍战武器”。

“震网”于2010年7月被发现，这种蠕虫病毒专门针对德国西门子公司设计制造的供水、发电等基础设施的计算机控制系统，伊朗曾承认“震网”影响到其核电站的部分离心机。Duqu病毒针对的也是工业控制系统，目的在于收集信息。

从功能上看，“震网”和Duqu能破坏某个目标，而“火焰”则是为了收集各行业的敏感信息。

位于日内瓦的国际电信联盟说，“火焰”是危险的间谍工具，可以用于攻击关键的基础设施。这是该组织目前发出的最严肃的警告。

伊朗国家计算机紧急情况应对小组推断，“火焰”入侵是一次间谍破坏行动。

卡巴斯基实验室安全问题高级研究员罗埃尔·斯霍文伯格说，从规模上看，这种新式武器是此前出现的网络炸弹的20倍，其威力也大得多。因此实际上已自成一支军队了。他说：“‘火焰’在实施网络间谍活动。”

谁制造的 ▶ 伊朗怀疑美以所为

伊朗怀疑以色列参与设计了该病毒。以色列分管战略事务的副总理摩西·亚阿隆5月29日说，以“火焰”等电脑病毒发起攻击等方式阻止伊朗核活动的做法合理。不过，以方官员5月31日否认以与这一病毒有关。

有伊朗媒体指出，“火焰”病毒可能在5年前甚至8年前即被激活，美国和以色列具备设计“火焰”病毒的能力，利用电脑病毒攻击伊朗关键行业及核设施系统是西方应对伊朗核计划的手段之一。

卡巴斯基实验室认为，“火焰”病毒自2010年3月起“猖獗”，由于其结构的复杂性和攻击目标具有选择性，安全软件一直未能发现它。

不少技术人员推测，从“火焰”病毒的复杂结构和广泛攻击范围看，该病毒背后可能有某国官方机构支持。 **据新华社等**

◓链接

“火焰”病毒已入侵我国

据新华社北京6月1日专电 “席卷全球的‘超级火焰’病毒已入侵我国”，知名网络安全企业瑞星公司就此发布红色安全警报，并提醒企事业单位高度重视此病毒，积极做好安全防范工作。

分析显示，“超级火焰”病毒相比去年肆虐全球的“超级工厂”病毒更为复杂，危害性更高，政府机构、大型企业一旦感染，将迅速蔓延，面临机密信息泄露的风险。

◓延伸

美军“奥运会”攻击伊朗核设施

据美国《纽约时报》报道，美国总统奥巴马从任职开始，就密令加快对伊朗主要铀浓缩设施计算机系统进行网络攻击。

这个攻击计划早在前总统小布什任内就开始进行，代号为“奥运会”，奥巴马上台后决定加快对伊朗核设施网络战的进攻步伐，

2010年夏季，由于一个程序错误，美国与以色列专家研制的一个蠕虫病毒“Stuxnet”意外脱离伊朗纳坦兹核电站，而散播到全世界的互联网系统。这个事件导致美国网络战计划泄露天机。

在接下来数周内，伊朗纳坦兹核电站被一波又一波的电子蠕虫病毒击中。伊朗近1000个离心机一度瘫痪。

报道称，这是美国首次多次使用网络战武器瘫痪他国的基础设施。根据参与“奥运会”计划决策会议的官员透露称，奥巴马对美国投入新领域进攻武器知之甚详。 **（钟欣）**

统筹：崔京良
美编：宫照阳 组版：陈 华