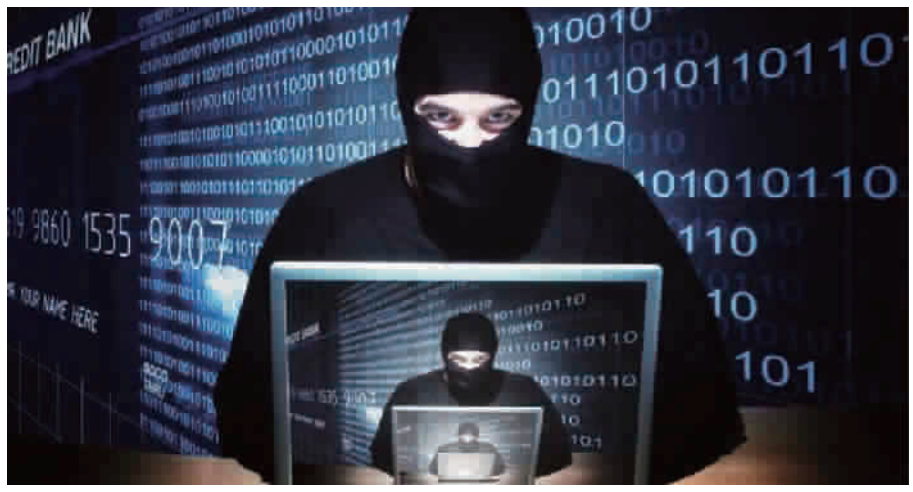
骇客到处找 网上高价卖 恐怖新袭击 可能网上来

程序漏洞：网络战争“军火”

网络战争曾经只是科幻小说题材，如今已成现实。

一场号称“零世界大战”的战争就这么打响了。注意，这不是发生在遥远未来的科幻故事，而是业已存在、每天都在上演的剧目。

这是一场硝烟四起的战争：互联网是战场，程序漏洞是军火，骇客是军火商，个人、企业和国家在其中打得难辨敌我。



■『超级骇客』随时在网上寻找程序漏洞

大学辍学后，美国青年阿龙·波特努瓦投身一个新兴行业——发现并出售程序漏洞，为此成立了一家名为“智识外逃”的公司。

这家公司的9名员工几乎全是“超级骇客”，他们的日常工作就是攻击目标软件，寻找侵入系统的办法。他们的目标包括浏览器、电邮客户端、即时通讯客户端、Flash、Java、工业控制系统，以及任何可以被攻击者当作突破口的东西。

错误成为昂贵商品

这是一个赚钱的营生，畅销软件或操作系统的漏洞一经发现，倒手买卖之后价值飙升，价格达数百至数万美元不等。微软和谷歌等技术企业每年都砸下数百万美元，重金悬赏查找自己公司的程序漏洞。

一旦发现某个漏洞，“智识外逃”公司的研究人员通常会起草一份专业报告和技术文件，说明这个漏洞是什么、在哪里、如何发现、在什么版本的软件上运行以及如何修复等信息。

最重要的是，“智识外逃”会告诉你如何激活并利用这个漏洞。购买他们的漏洞需要注册成为会员，年费在20万美元左右。

“智识外逃”的客户基本分为两类：攻击型和防守型。安全公司和反病毒软件开发商属于防守型，他们获取产品相关信息、为客户提供有关系统威胁的最新信息。攻击型客户则包括侵入测试者，他们买下“零日漏洞”模拟攻击自己或他人网络。

“零日漏洞”是一个专业术语，指漏洞的新鲜程度，即公开时间为零天、尚无人尝试修复的漏洞。

在这个不大的精英领域中，还有总部位于法国南部的Vupen公司、马耳他的Revuln公司、美国的Netragard公司和加拿大的Telus公司。Netragard公司的口号是：“我们保护你们不受我们这种人的攻击。”

程序漏洞说白了就是编程中出现的错误和纰漏，却摇身一变成为价格不菲的商品，还催生出一个全新产业。这与我们所处的计算机时代不无关系。

随着计算机的高度应用，现实生活几乎全部数据化。商业活动、医疗记录、社会生活和政府行为变为一节节数据，录入由软件构成的计算机内核。这些数据令人垂涎，既有间谍也有罪犯，既有政府也有企业，程序漏洞则是猎取数据的武器。

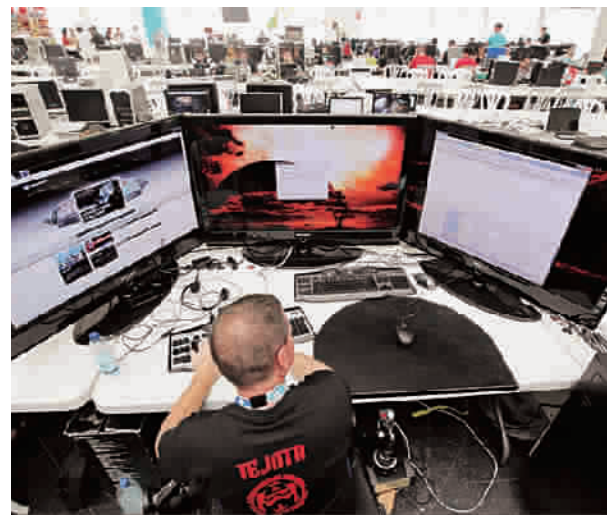
特殊武器威力巨大

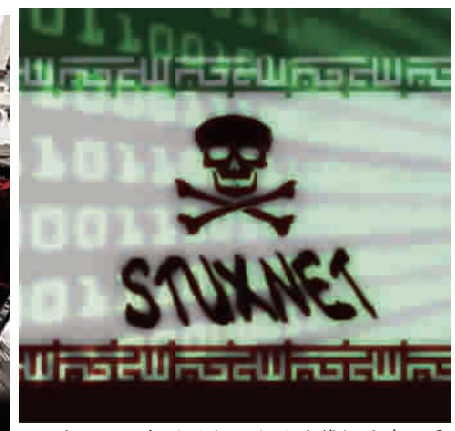
几年前，美国和以色列联合研发了计算机病毒“震网”（Stuxnet），堪称第一件真正的网络武器。一名双重间谍携带写有这种病毒的U盘，来到伊朗纳坦兹市某处正进行铀浓缩的核设施。在这里，他把U盘插入计算机，把病毒植入系统。

查看整个计算机系统后，“震网”向其美国和以色列主人传回详细情报，随后开始大规模侵入控制离心机的计算机，最终导致大约两成离心机陷入瘫痪。

“震网”威力巨大，全凭借系统漏洞得以施展。据分析，“震网”至少利用了4个不同的系统漏洞，包括一个微软视窗操作系统的漏洞，才得以侵入伊朗离心机的计算机系统。

这些漏洞，或者更确切地说，利用这些漏洞所需的知识，好比虚拟世界中制造核武器的浓缩铀，是昂贵且精密的武器，是极端复杂的武器系统核心。因为这些漏洞的存在，“震网”极具杀伤力，从纳坦兹市的核设施扩散开来，导致全球大约10万台计算机受感染。





▲ 美国和以色列联合研发的计算机病毒“震网”（Stuxnet）威力巨大

◀ 在网络时代，程序漏洞可能造成重大损失

■ 美国军方频繁利用程序漏洞对他国发起网络攻击

“自由市场”存在隐患

现实世界中，战斗机和地雷等军火交易有着严格控制。网络军火——程序漏洞的买卖则是一片罕见监管的“自由市场”，卖给谁、不卖给谁，全凭骇客说了算。

目前，漏洞市场的行为仍依赖自愿和自律原则。波特努瓦及其团队表示，他们尽量不涉及政治。然而，无论“智识外逃”还是其同行Vupen等公司，都恪守沉默原则，不追问“零日漏洞”将侵入谁的计算机、为何侵入。

真正的末日场景是“零日漏洞”落入恐怖组织之手，用于攻击公共设施，那将是一场真正的梦魇。

以“数据采集与监视控制系统”（SCADA）为例，这个控制工业系统的软件系统就是“震网”病毒攻击的目标。美国联邦调查局（FBI）负责网络和特殊行动的前特工玛丽·加利根说，一旦恐怖分子发现公共设施网络的漏洞，后果不堪设想。“我们能想到的一切工业系统，制造车间、电网、供水或电梯，都由与互联网连接的数据设备运行。令人担忧的是，这是保护力度最弱的环节。”

更糟糕的是，哪怕不能在公开市场上获得程序漏洞，不法分子也能从活跃的“漏洞黑市”上购买。兰德公司在报告中指出，“漏洞黑市”已成为“竞技场”，参与者是“一些受金钱驱使、具高度组织性和复杂性的组织”。

波特努瓦则对“漏洞黑市”嗤之以鼻。他说，黑市上的大部分漏洞都不具备“新鲜度”。犯罪分子通常瞄准已推出安全补丁的老旧漏洞，找那些尚未更新软件的计算机下手。

战争必将旷日持久

当然，最理想的情况是使用完美无瑕的软件。然而，这在现实中绝无可能。计算机应用越普遍，软件就越复杂，漏洞也越多。

以一台个人笔记本电脑为例，其操作系统由数千万行代码组成，安装的应用软件大多数仅完成四分之三就匆匆上市。如果再与手机、平板电脑等其他设备连接，形势将迅速失控。

人类打造了互联网，却难以控制其中的信息流动。这是一场新的战争，虽然并不引人瞩目却旷日持久。这场战争模糊了军事与民事、个人与公共、政治与商业的界限，受害者损失的是个人数据和知识产权。

正如美国政府一名高级官员所言：“程序漏洞将一直存在，人们必须生活在这种假设之下：有时候，坏人会侵入。”

袁原

相关链接

科技企业悬赏 查找程序漏洞

想要修复所有漏洞就好似妄想排干海洋。无论编码水平如何提高，都不可能永远消除程序漏洞。

目前，美国国家漏洞数据库列出63239个漏洞。去年，研究人员平均每天发现13个漏洞。今年3月，美国联邦政府通报，去年共有3000家美国企业遭到黑客攻击。

越来越多技术企业意识到，与其让自己的编程员查找漏洞，不如重金悬赏查找。

1995年，美国网景通信公司（Netscape）推出“漏洞奖金”项目，为找出该公司浏览器漏洞的人提供现金奖励。

2010年，谷歌公司推出奖励发现Chrome浏览器漏洞的计划。今年，谷歌用于该计划的支出累计达到330万美元。

微软公司对视窗操作系统严重漏洞发现者的奖金最高达到10万美元。

去年，脸谱公司为687个程序漏洞支付了150万美元的奖金。

程序漏洞市场 美国政府活跃

程序漏洞的杀伤力巨大，如果应用得当，威力甚至不亚于核武器，因此越来越多的人开始关注漏洞市场。

2002年，美国信息防护公司（iDefense）开始购买各种程序漏洞。2005年，TippingPoint公司也推出了类似的购买计划。

程序漏洞买卖是一个交易活跃且混乱的市场，出价最高的买家往往令人生疑。相比之下，信息防护公司和TippingPoint比较可靠。他们好似回收放射性废物的“零日漏洞”的“处理厂”。从骇客或他处购得漏洞后，这两家公司会提醒客户予以警惕，并与软件开发商合作修复。

还有的企业成为承包商，专门向政府出售程序漏洞。多年来，总部位于华盛顿特区的Endgame公司向美国政府出售漏洞，被《福布斯》杂志称为“骇客领域的黑水公司”。

美国政府一直活跃在这个市场上。《华盛顿邮报》分析斯诺登泄密文件发现，美国国家安全局预算中，有2510万美元用于“额外秘密购买软件漏洞”，还有6.52亿美元用于代号GENIE的秘密计划，任务是在外国计算机网络上植入恶意代码。

截至2013年底，GENIE已经控制全球大约8.5万台计算机。2015年美国国防预算中，更有50亿美元用于网络空间行动，但具体去向没有公开。

斯诺登提供的机密文件显示，2011年美国对中国、俄罗斯、伊朗和朝鲜等国家发起了231次网络攻击。这还只是2011年的数字。美国方面的数据则显示，普通美国企业在2013年对近1.7万起网络袭击提起诉讼。