电脑系统专家： 入侵不同网站手段不一 黑客从“人”和“机器”下手 网上用假名犯法 身份同样会被查出

November 16, 2013 by sgfactblog

黑客入侵网站和电脑系统的手法越来越复杂，而且会针对不同的目标，采用不同手法持续攻击。他们也会找出有防御漏洞的网站，逐一展开攻击。网络安全专家警告，黑客轻则盗取个人资料，重则可能威胁国家安全。

黑客主要从“机器”和“人”两方面下手。前者是通过互联网把最新型的间谍软件（malware）直接侵入一家公司或机构的电脑系统内。

杀毒软件开发商趋势科技公司新加坡区经理佘仰明受访时指出，一般电脑杀毒软件是靠辨认间谍软件的特征进行探测和扫除。软件开发商发现新间谍软件后的一段时间，才更新特征数据库。在这之前，杀毒软件无从辨认和抵抗新的间谍软件。

在针对“人”的攻击方面，黑客一般会锁定公司高层职员，因为这些职员会处理机密文件。黑客会发送电邮骗该职员打开假网页，再通过假网页把间谍软件植入职员的电脑，进而入侵公司的电脑系统。若间谍软件成功入侵公司电脑系统，即使后来被发现，也很难去除。操控恶意软件的黑客就能远程窃取公司资料、职员密 码和机密文件等。

网络攻击有难度之分

佘仰明说：“韩国政府和机构、社交网站、提款机盗取款项案和最近被黑客入侵的本地网站，都是具针对性的攻击。”

网络攻击也有难度之分，最简单的是用间谍软件向特定人物骗取资料。难度较高的是发掘系统漏洞，暗中盗取密码。

最严重的相信是以普通电脑活动为掩护，在暗地里展开一系列攻击。一般防御系统无法探测出这类入侵方式。

佘仰明说，有的黑客抱有政治动机，有的只想窃取资料，但主要目的是用这些资料盗取银行存款、勒索资料拥有者或把资料转卖出去。以银行为例，若系统被入侵，损失的不仅是价值数百万元以上的客户资料，信誉也将毁于一旦。

赛门铁克公司的 2013 年《诺顿报告》显示，新加坡每个遭受网络攻击的消费者付出的成本代价平均为 1448 元，比去年多了 75%。

希腊外交部和欧洲安全与合作组织（Organization for Security and Co-operation in Europe）今年 10 月遭到黑客攻击，3700 份文件外泄，在在显示黑客的威胁无处不在。

许多新加坡人使用 Singpass 密码登录中央公积金局、建屋发展局等政府网站，因此，这一层面的网络安全极为重要。

赛门铁克公司新加坡区总监陈昱伟说，大家都应该抱着所有人都是被攻击目标的心理，不要以为公司或网站规模小或少人听闻，就掉以轻心。

他强调，网站和电脑系统的防御措施必须涵盖各方面，有些部分甚至得重叠。从网络系统的防御保护、时时更新防火墙到加强电脑病毒探测，都需要注意。

公司也需提醒职员提高警惕。他建议，公司为职员提供应对训练，深入了解资料泄露的严重性，避免落入黑客的陷阱。

黑客主要从“机器”和“人”两方面下手。前者是通过互联网把最新型的间谍软件直接入侵公司的电脑系统；后者则是锁定一般能接触公司机密文件的高层职员，发电邮骗他们打开假网页，进而入侵公司电脑系统。

联合早报 李蕙心
2013 年 11 月 16 日

网上用假名犯法 身份同样会被查出

本地网站数次被不同黑客盯上，网络专家指出，这种情况在国外屡见不鲜，许多黑客是跟风的抄袭者。

他们误以为在网络上不露真面目就可为所欲为，其实他们在虚拟世界犯法同在现实中犯法一样，都得付出代价。

宏茂桥市镇理事会网站、人民行动党社区基金网站、《海峡时报》博客及城市丰收教会创办人之一的何耀珊个人网站，过去几个月来相继被黑客侵入。随后总理公署和总统府网站也成为黑客的目标。

据保安方案公司安世科安防科技（Ademco）销售与市场营销总监林柏力分析：“在现实世界中干案，可能会留下指纹或被认出样貌；但在虚拟世界中，一些人、尤其是青少年误以为用虚假的名字就可掩饰错误的行为，当他们看到别人成功入侵网站后也想尝试。”

他指出，这些黑客用的是较简单的入侵手法，没想到成功入侵网站，这助长他们的胆量，但在虚拟世界也会留下犯法痕迹。若以日前被捕的黑客占姆士·拉杰为例，他涉嫌干案时人在国外，但身份仍被追查到。

比起骗取银行密码和机密文件，网站内容被篡改看似无伤大雅，但这给社会带来的影响可大可小。

林柏力说，黑客具有政治目的，他们在互联网上宣传的内容可能引发社会不安，事态可能一发不可收拾。“幸好，多数本地网民都能辨别网络内容的真伪，也不认同黑客的做法。”

青少年较容易受他人影响，他建议政府部门可考虑加大宣导网络安全意识的力度，教导青少年正确使用互联网的方式。