瑞星 2012 年上半年中国信息安全报告

北京瑞星信息技术有限公司

2012 年 7 月

免责声明

本报告综合瑞星“云安全”系统、瑞星客户服务中心、瑞星互联网攻防实验室等部门的统计、研究数据和分析资料，仅针对中国大陆地区 2012 年 1 至 6 月网络安全现状与趋势进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为互联网信息安全状况的介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，瑞星公司不承担与此相关的一切法律责任。

目录

报告概要

- 2012 年 1 至 6 月，瑞星“云安全”系统共截获新增病毒样本 3,349,373 个，其中木马病毒 2,808,723 个，占据总体病毒比例的 83.86%。 从表面上看，病毒疫情似乎处于“风平浪静”的状态，但实际上病毒将其破坏行为转变为“地下操作”，用户传统观念中的中毒后“电脑死机”、“无法上网”等现象不再是主流病毒采用的方式。64 位操作系统、苹果 Mac 操作系统均不断遭受病毒攻击，以往用户心目中相对安全的系统的概念不复存在。

- 2012 年 1 至 6 月，据瑞星“云安全”数据中心监测，截获到挂马网站(以网页个数统计)237 万个，与去年同期的 236 万个相比基本持平。2010 年、2011 年两年挂马网站连续下降 90%以上的态势到今年戛然而止，主要原因是挂马网站形式单一，且技术上无本质突破，安全厂商现阶段的防护技术可对其进行有效打击。
- 2012 年 1 至 6 月，瑞星截获钓鱼网站 314 万个(以 URL 计算)，是去年同期的 1.3 倍；共 9,903 万人次网民遭钓鱼网站侵袭。假冒银行、假冒中奖信息、假冒购物网站仍然占据着钓鱼网站“头三把交椅”，金融行业成为黑客攻击的重灾区。上半年数据显示，彩票类钓鱼网站成为黑客新宠，同时节假日及热点事件成为黑客们关注的焦点。
- 随着移动互联网的迅速发展和智能手机的大面积应用，在给广大用户带来方便的同时也带来了巨大的安全隐患，在移动互联网的三大平台 Android、IOS、Symbian 中，Android 系统由于其开放性较高，业已成为黑客攻击的主要目标。据瑞星“云安全”数据监测显示，仅今年上半年就截获 Android 病毒样本 4,252 个，其中功夫熊猫系列病毒最为猖獗。
- 上半年国内企业信息安全事故的频发，企业网站、电子商务网站及政府信息网络均曾遭到不同程度的攻击，部分知名网站甚至出现大规模的数据泄露，导致用户和企业的利益严重受损，企业级、国家级信息对抗已升级至“核战”等级，近期爆发的“超级火焰”病毒就是最典型的代表。
- 瑞星预计，下半年中国信息安全状况仍将动荡不安，挂马、网络钓鱼等威胁凸显。报告分析认为，这些恶意行为几乎全部是受经济利益的驱使。而个人隐私安全仍然堪忧，不法分子千方百计窃取用户的隐私信息。另外，瑞星专家预计，规模更大、技术更先进的大型网络攻击，在今后有可能愈演愈烈。

一、病毒与木马

1. 病毒概述

2012 年 1 至 6 月，瑞星“云安全”系统共截获新增病毒样本 3,349,373 个，病毒总体数量与去年同期相比有所下降。其中木马病毒 2,808,723 个，占据总体病毒比例的 83.86%，紧随其后的病毒依次为感染型病毒(Win32)、蠕虫病毒(Worm)、恶意广告程序(Adware)、病毒释放器(Dropper)和黑客后门(Backdoor)。

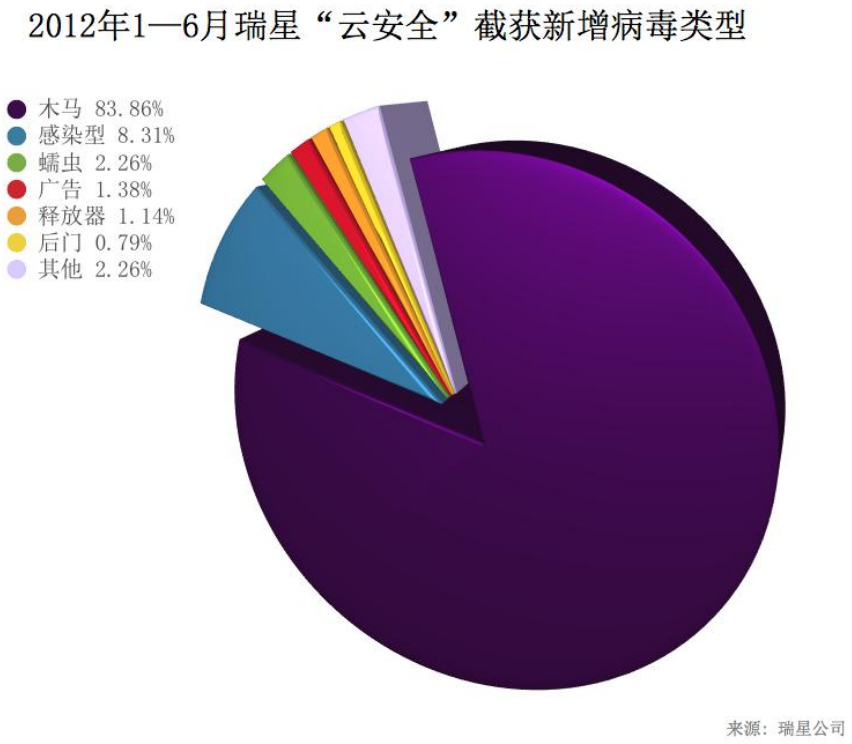

图 1：2012 年 1-6 月病毒构成分析图

2. 十大病毒排行：木马病毒猖獗

2012 年 1 至 6 月，共计 7.4 亿人次网民被病毒感染，平均每天 411 万人次网民中毒，按感染人数、变种数量和代表性进行综合评估，瑞星评选出了 2012 年上半年的十大病毒。

瑞星2012年1—6月病毒排行Top10

排名	病毒名称	病毒描述
1	Trojan.Script.JS.Pop.a（脚本木马病毒）	JS脚本，中毒后电脑出现恶意弹窗，增加恶意网站流量
2	Trojan.Win32.FakeIME.d（木马病毒）	病毒通过伪造成输入法入侵电脑，进行盗号行为
3	Worm.Win32.FakeFolder.c（蠕虫病毒）	病毒伪装成文件夹图标迷惑用户，中毒后会篡改IE主页为恶意网站
4	Trojan.DL.Win32.AVPlayer.a（木马病毒）	病毒为木马与黑客后门功能于一身，盗取用户电脑隐私信息
5	Hack.Exploit.Swf.a（漏洞利用脚本病毒）	利用系统漏洞入侵电脑，从黑客指定网站下载其他病毒
6	Trojan.Win32.Fednu.dba（木马病毒）	释放黑客后门并运行，接受远程命令，使中毒电脑成为肉鸡
7	Trojan.Win32.Fednu.axe（木马病毒）	连接黑客服务器，上传本机数据，接受黑客命令盗取隐私
8	Trojan.Win32.Generic.12B9CBFF（木马病毒）	淘宝客劫持病毒
9	Trojan.DL.Win32.NewLoader.b（木马病毒）	下载者，从指定网站下载病毒并执行
10	Worm.Win32.TaopuLS.a（蠕虫病毒）	伪装成文件夹图标，诱骗用户点击，释放后门

来源：瑞星公司

图 2：2012 年上半年十大病毒

3. 病毒技术趋势分析：从“破坏”到“谋财”

通过对 2012 年 1 至 6 月新增样本的病毒行为分析发现,今年的病毒数量与去年同期相比有所下降，从表面上看，似乎处于“风平浪静”的状态，但实际上病毒将其破坏行为转变为“地下操作”，用户传统观念中的中毒后“电脑死机”、“无法上网”等现象不再是主流病毒采用的方式。目前，最为流行的病毒均以篡改 IE 首页、盗取用户隐私信息等方式，实现为黑客带来巨大经济利益的目的。

1)病毒、杀软“战争”进入白热化

随着杀毒软件对病毒的强力围剿，病毒作者对抗杀毒软件的方法也不断升级。以往，病毒通过增加垃圾数据将病毒文件不断增大来规避“云查杀”，今年已升级为通过病毒守护进程，定时更新病毒 MD5 值的方式，使杀毒软件无法进行有效识别。瑞星安全专家介绍：“这种方式就好比汽车的自动翻牌器一样，在遇到检查时，自动换上另一套号牌。”

此外，某些病毒竟然能够做到使杀毒软件“选择性失明”。传统病毒在进入系统后，为躲避杀毒软件查杀，往往会利用各种手段，尝试将其破坏，这种方式容易引起用户和安全厂商的注意，从而察觉电脑中毒。因此，病毒作者进行了策略调整，借助一些正常软件的数字签名，“合法化”的绕过杀毒软件的检测机制，使杀毒软件不将其视为病毒，而是当作“正常软件”放行。

例如，瑞星“云安全”系统近期监测到一款名为 Trojan.Win32.FakeIME 的病毒，该病毒将自身伪装成为某知名输入法图标，并盗用其数字签名，从而逃避杀毒软件的监控和查杀。瑞星安全专家介绍，病毒采用的技术在进步，杀毒软件的查杀技术也在不断提高。预计今年下半年，病毒和杀毒软件的对抗将会向白热化升级。

2)网银盗号愈演愈烈，病毒趋于智能化

随着网上购物、网银交易的不断普及，大批黑客开始专注劫持网银进行获利。2012 年上半年，瑞星“云安全”系统智能分析处理中心经过对流行病毒行为方式自动提取规则后发现，针对网银类的木马病毒使用的技术发生了明显变化。

以最为知名的“网银超级木马”为例，最初的样本往往采用恶意 DLL 文件实现篡改支付信息的方式，如今发展到通过解密并将恶意代码注入到傀儡进程中，由傀儡进程去实行恶意行为，这样做的目的是能够绕开一些杀毒软件的主动防御规则，从而逃避查杀。

如图所示，最初“网银超级木马”和近期最新变种行为流程对比图：

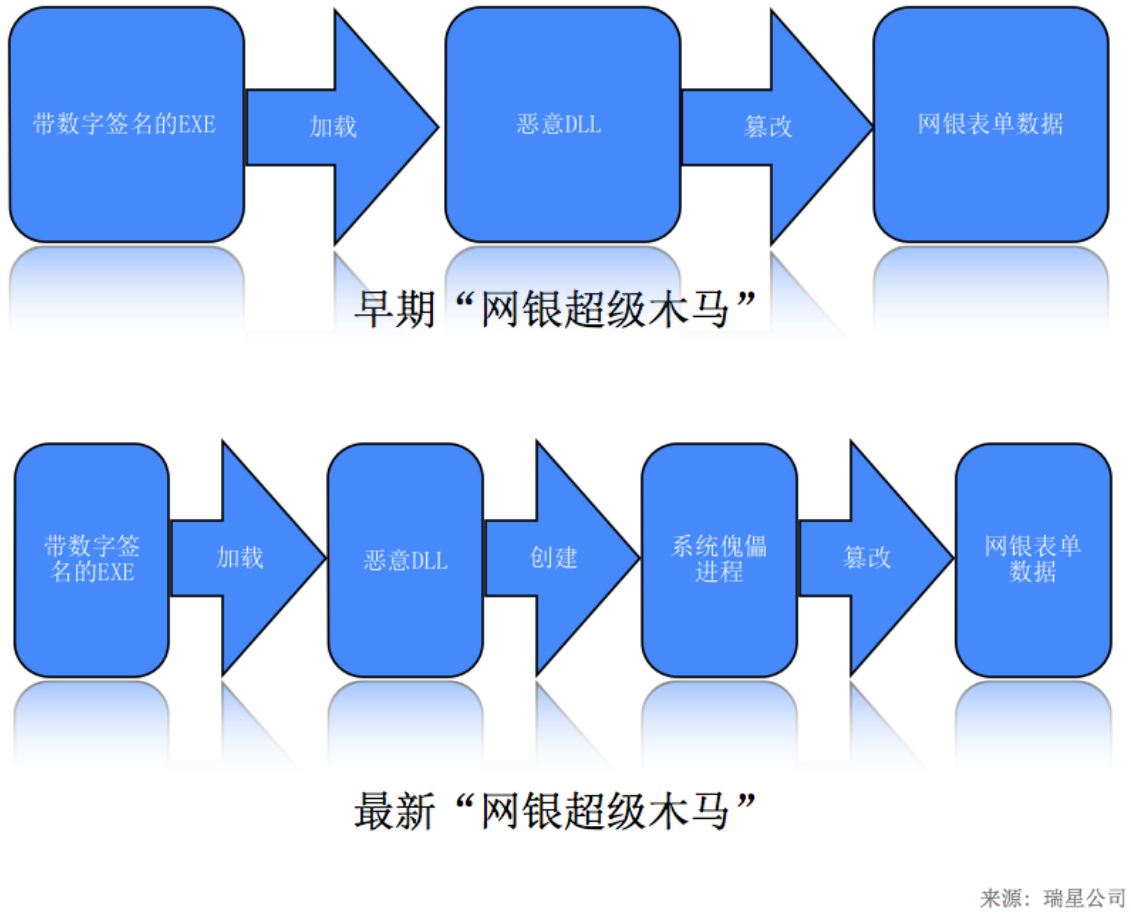

图 3：“网银超级木马”最新变种行为流程对比图

3)感染型病毒蔓延，64 位操作系统不再安全

通过对 1 至 6 月的数据分析发现，感染型病毒*依旧是继木马之后的第二大病毒类型。另外，随着 64 位操作系统的逐渐普及，感染 64 位 PE 文件的病毒呈明显上升趋势，这意味着 64 位操作系统已不再安全，尤其是企业级用户应采取相应的安全保障措施，才能预防此类信息安全威胁。

上半年，一种可感染 64 位操作系统的“Xpaj”病毒悄然流传，“Xpaj”比以往所有感染型病毒都要复杂，不仅使用了传统的入口点模糊、多态等技术，最为复杂的地方是它将病毒代码替换掉原程序中子函数的代码，从而与原程序代码很好的融为一体，给传统杀毒软件在清除

该病毒时造成了巨大的困难，“不是杀不了，就是杀后被感染文件无法使用”。

**注释：感染型病毒具有易传播，不易清除等特点，同时会给用户造成巨大的危害。传统的普通感染型病毒如:在文件末尾增加节、增加最后一个节大小、修改 PE 文件入口点。针对这种普通感染型病毒，传统杀毒软件比较容易清除干净，但是新型的复杂的感染型病毒业已出现。*

4)Mac OS X 安全优势不在，苹果用户安全意识需加强

苹果曾经自豪的宣称其开发的 Mac OS X 操作系统不易受病毒攻击。然而近期，苹果在网站上移除了“Mac 不会感染 PC 病毒”和“保障你的数据安全，什么也不用做”的说法，其原因是苹果 Mac 电脑近期遭到 Flashback 僵尸网络的攻击。这使苹果意识到，自己的系统也并不像预想的那样百毒不侵。

瑞星安全专家指出，世界上没有绝对安全，只有相对安全。用户之所以认为 Mac 系统安全性高，是由于此前的用户数较 Windows 相差甚远。随着近年来，苹果产品在中国用户中的迅速普及，黑客针对该系统的入侵价值大大提升，因此，Mac 安全问题才显露出来。未来这种情况还可能继续升温，广大用户需要提高安全意识。

二、恶意网站

1. 挂马网站：常用操作系统频遭攻击

1)挂马网站概述

2012 年 1 至 6 月，据瑞星“云安全”数据中心监测，截获到挂马网站*(以网页个数统计)237 万个，与去年同期的 236 万个相比基本持平。2010 年、2011 年两年挂马网站连续下降 90%以上的态势到今年戛然而止，主要原因是挂马网站形式单一，且技术上无本质突破，安全厂商现阶段的防护技术可对其进行有效打击。

令人欣喜的是，在报告期内瑞星拦截挂马网站的攻击总计 1,986 万次，与去年同期 5,430 万次相比降低 65.43%。其具体分布情况如下：

图 4：2012 年 1-6 月挂马网站上报量

**注释：挂马网站指的是被黑客植入恶意代码的正规网站，这些被植入的恶意代码，通常会*

直接指向“木马网站”的网络地址。木马网站：是一种利用程序漏洞，在后台偷偷下载木马的网页。这些网页通常放在黑客自己管理的服务器上，当用户访问时，会把许多木马下载到用户机器中运行。

2)Windows 相关漏洞仍难摆脱挂马网站的“魔咒”

经瑞星监测，上半年的木马攻击有 4 成基于 IE 漏洞，4 成基于 Flash 漏洞，2 成为其他漏洞。Windows 操作系统的相关漏洞仍然是被黑客们利用最多的主要攻击途径。

瑞星2012年1—6月漏洞排行Top10

排名	漏洞编号
1	CVE-2010-0806（IE漏洞）
2	CVE-2012-0003（IE漏洞）
3	CVE-2011-1255（IE漏洞）
4	CVE-2011-0611（Flash漏洞）
5	CVE-2011-2140（Flash漏洞）
6	CVE-2012-0754（Flash漏洞）
7	CVE-2011-3544（Java漏洞）
8	CVE-2011-0618（Flash漏洞）
9	CVE-2011-2950（RealPlayer漏洞）
10	CVE-2006-0003（IE漏洞）

来源：瑞星公司

图 5：2012 年 1-6 月漏洞排行 Top10

3 月 13 日晚间，微软发布了今年 3 月份的安全公告，该公告中共更新了 6 个漏洞，其中一个名为 MS12-020 的漏洞为超高危漏洞，黑客可利用该漏洞构造特殊的 RDP 协议包远程控制用户电脑或服务器。由于该漏洞影响 XP、2003、Win7 和 2008 等所有 Windows 系

统，所以给用户的隐私安全造成严重的威胁。

而时隔一个月，4 月 25 日，存在于微软刚刚发布一个名为 CVE-2012-0158 的漏洞被披露已经被黑客利用。黑客利用该漏洞制造出畸形的 doc/rtf 等文件，通过电子邮件、网页等形式传播，用户一旦打开，电脑就会被黑客控制，盗取隐私信息、下载病毒。

2. 钓鱼网站：种类多样化，诈骗手段层出不穷

1)数据分析

2012 年 1 至 6 月，瑞星截获钓鱼网站 315 万个(以 URL 计算)，是去年同期的 1.3 倍；共 9,903 万人次网民遭钓鱼网站侵袭。具体分布情况如下：

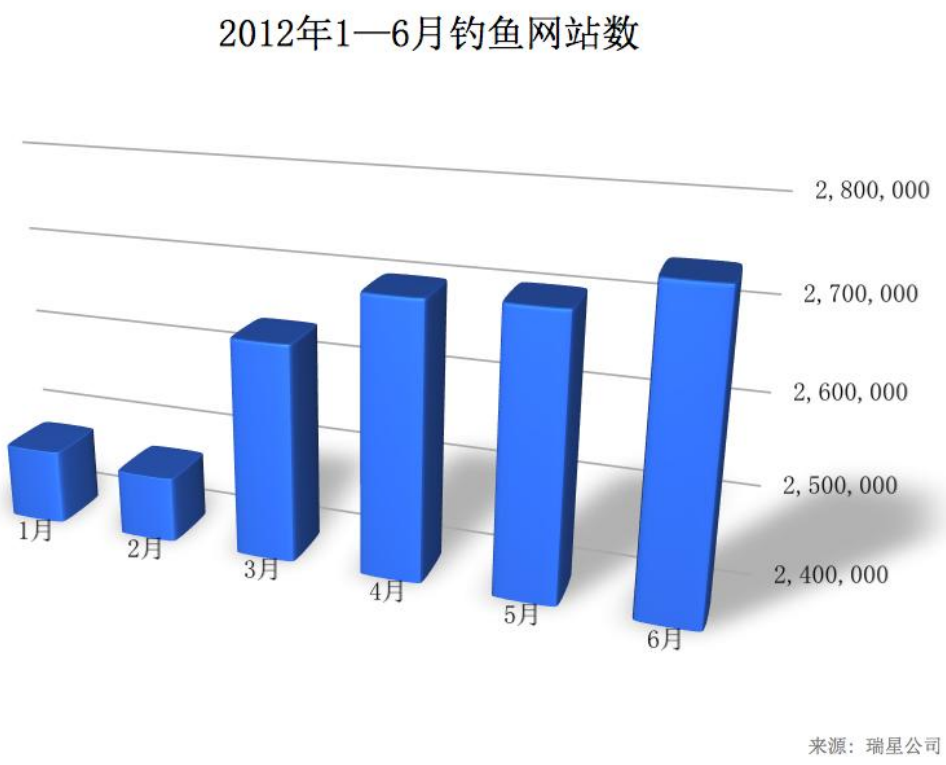

图 6：2012 年 1-6 月钓鱼网站数

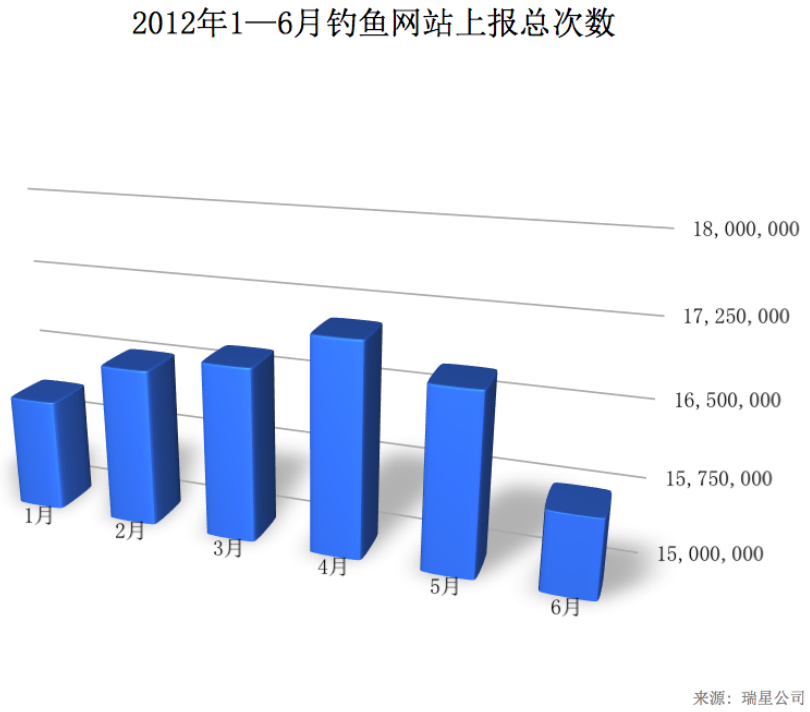

图 7：2012 年 1-6 月钓鱼网站上报总次数

钓鱼网址大量增加，而网民受到钓鱼网站攻击次数却小幅回落，其原因在于现有的反钓鱼技术能够拦截大多数钓鱼网站，并通过“云拦截”、“云防护”等手段第一时间让所有用户具有智能反钓鱼能力。上半年钓鱼网站最多的类型分别为：假冒银行类、假冒中奖信息类、假冒购物网站类。详细情况如下：

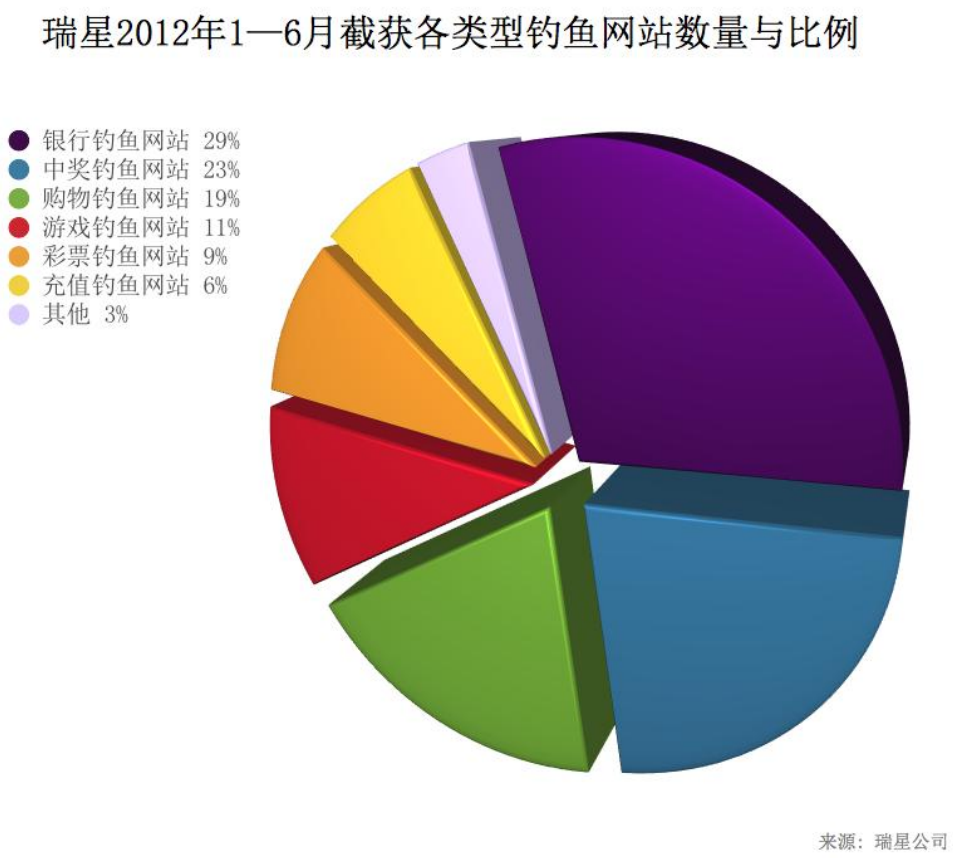

图 8：2012 年 1-6 月钓鱼网站数量与比例

2)网络钓鱼现状分析

据瑞星“云安全”数据监测显示，上半年，随着 B2C 电子商务的迅猛发展，网络钓鱼事件愈加频繁。钓鱼网站的生命周期比去年同期更短，多数都是跟随节假日以及热点事件应运而生。同时，对比去年同期数据，网络钓鱼类型在构成上也更加复杂，说明黑客也在根据市场的变化不断调整策略。

A. 银行类网站频遭仿冒

目前，银行类网站仍然是钓鱼网站最常见仿冒对象之一。相对于其他类型网站，假冒银行网站窃取用户信息更加直接，同时给用户带来的经济损失也更加巨大。

今年上半年，网上曝出中国银行网站频遭大量钓鱼网站假冒，假冒网站通过诈骗短信谎

称中国银行网银升级，进而骗取客户的密码。仅仅几十秒时间，就能转走受害人存款，多的有数百万元之巨。

B. 中奖信息类、假冒购物类钓鱼网站大肆横行

中奖信息类钓鱼网站、假冒购物类钓鱼网站往往都是利用一些网友贪占小便宜的心理进行诱骗。近期，这些网站甚至掌握了一些知名品牌或企业的网上活动周期，对各方面活动信息都模仿的惟妙惟肖，让网友们难以分辨真假。

一位李小姐就表示曾经收到过 QQ 中奖的邮件。网页中有 QQ 的 LOGO 以及详细的兑奖步骤，按照提示填写了个人资料以后，该网站就要求李小姐填写自己的银行账号及密码。这使李小姐警惕起来，仔细一看，网页显示的地址并不是腾讯公司的官方页面，而是 www.qquuccqq.com。

来源：瑞星公司

图 9：骗子发送的钓鱼邮件，实际上腾讯根本不会通过邮件发布此类消息

C. 彩票类钓鱼网站激增

今年上半年，彩票类钓鱼网站数量猛增，从去年的寥寥无几增加到总体钓鱼网站数量的9%。近年来，线上购买彩票已经成为网友们习以为常的事情，一些专业的“彩民”甚至会一次性花上千乃至上万元投注，这也给了黑客们可乘之机。

经瑞星“云安全”数据中心监测，今年4月份，彩票类钓鱼网站激增，这些钓鱼网站都是模仿正规彩票网站，骗取“彩民”们的信息及钱财的。

北京的张先生就表示曾在彩票网站投注时被骗过 2 万余元。张先生本是跟别人合伙对彩票进行“投资”的，没想到在进行操作的时候误点入钓鱼网站，白白损失了钱财的同时，还将合伙人得罪了，可谓是有苦说不出。

D.节假日成为钓鱼高峰期

据今年上半年统计，节假日是钓鱼网站最猖獗的时期。由于近年来，商家惯于利用各种节假日进行网上促销等活动，这让黑客们有机可乘。春节、三八妇女节、五一、母亲节、端午节、父亲节，消费者已经习惯在这些节日进行采购，无论是自用还是送礼，这个时期的折扣多，非常有诱惑力。而黑客们正是看中了这一点，以节日低折扣的招牌，混在诸多网购网站当中，骗取网友的信息与钱财。

E. 热点事件催生网络钓鱼

近年，在网络运营商们从追捧热点事件中看到了商机的同时，黑客也想借机谋取不义之财。高考前夕，各种“绝密”考试资料网站如雨后春笋般冒头。考生家长王女士透露，曾经在网上为孩子购买复习资料，网站推销说该资料能够百分之八十压中考题，然而当王女士用网银向其打款后，购买的考试资料却迟迟没有收到，再联系网站客服的时候，发现该网站提供的联系方式是假的。

无巧不成书，近期欧洲杯开幕，根据瑞星“云安全”系统数据分析发现，仅 6 月 9 日-11 日开赛的前 3 天时间内，瑞星就截获了 42 万个来自钓鱼网站的攻击，其中赌球类钓鱼网站更是高达 15%以上。这是因为很多对看球意犹未尽的网友在赌球网站上寻找刺激，参与了

网上赌球的活动，其带来的直接结果就是巨大的经济损失。

3)钓鱼网站趋势分析

通过上半年的现状分析，可以看到，目前黑客采取的钓鱼策略主要有两种，一种是直接仿冒网上银行交易系统，无论是银行类钓鱼网站还是购物类钓鱼网站，均属于此种范畴。另外一种是制造虚假信息，诱使网友进入专门制作的相关页面进行钓鱼，中奖类钓鱼网站就是其典型例子。

可以预见，在今年下半年，还将有更多的钓鱼网站崭露头角，而且极有可能会根据节日、重大时事热点，变化出新的花样，甚至运用一些新的手段。网友要提高警惕，擦亮自己的眼睛，尽早做好防护准备，对于普通广大用户而言，最直接有效的方式是安装一款具有智能反钓鱼功能的安全软件。

三、移动互联网安全

近年来，移动互联网发展迅速。智能手机的大面积应用，使得用户可以随时随地用手机收发邮件、购物、交费等。移动互联网市场已经显露出它巨大的价值。目前，移动互联网的三大平台分别是 Android、IOS、Symbian，相较于 IOS 及 Symbian 而言，Android 系统由于开放性较高，成为黑客主要攻击目标。

1. Android 病毒已成为用户的最大威胁

1)上半年 Android 中枪无数

据瑞星“云安全”数据监测显示，仅今年上半年就截获 Android 病毒样本 4,252 个，其中功夫熊猫系列病毒最为猖獗。该病毒是现在流传最为广泛、威胁性最高的 Android 病毒。病毒通过伪装成普通的手机软件，诱骗用户下载，一旦进入手机，就会在后台偷偷运行恶意程序。通常，被功夫熊猫感染的手机会出现手机无需解锁直接进入主菜单的症状。该病毒可以控制 Android 上所有软件，并控制整个系统分区，进而对手机做任何事情，甚至让手机永久报废。

Android 是一款开源的手机操作系统，由于其开放性高，应用广泛，同时它的漏洞也更容易被黑客们发掘、利用。用户一旦中毒，手机将被恶意扣费，隐私也将遭泄漏，并很可能遭受恶意推广等。随着移动互联功能的逐渐丰富、强大，这些病毒也将不断升级，带给用户的威胁将越来越高。

2)安全软件遭病毒“劫持”

最近已有基于 Android 平台的病毒可以在入侵系统的同时，攻击用户手机安全软件，让其失去防御能力。目前，瑞星手机安全软件已有专门针对此类病毒的查杀功能。

此类病毒的出现，意味着手机病毒将进入一个更加复杂的阶段，今后的病毒可能不再是简单的恶意扣费行为，而有可能更进一步，在劫持杀毒软件的同时，附加多种恶意行为，使

黑客盗取用户信息更加容易。移动互联用户将面临前所未有的更巨大的信息安全恐怖袭击。

2. 无线公共网络或成为泄密源头

随着无线网络应用范围的不断扩大，很大一部分的公共场所都提供了免费的无线网络接入服务，许多手机用户为了省钱就会加入这些免费 WiFi 网络当中，一些黑客就是利用这一点，伪造公共网络，并记录用户所有的操作信息。用户很难区分接入网络的真假，一旦连入“黑网”，黑客立刻就可以窃取手机上网用户的个人信息和密码，包括网银密码、炒股账号密码等。

目前，这种来自无线公共网络的攻击还处于萌芽阶段。但是有黑客声称：只要一台 Win7 系统电脑、一套无线网络及一个网络包分析软件，设置一个无线热点 AP，就能搭建出一个假冒公共网络。这意味着假冒一个公共网络是一件极其简单的事情，未来可能有更多心怀不轨的人利用这些简易的设备窃取手机用户的个人隐私信息，使用户遭受重大的经济损失。

四、企业信息安全

2012 年上半年国内企业信息安全事故频发，企业网站、电子商务网站及政府信息网络曾遭到不同程度的攻击，部分知名网站甚至出现大规模的数据泄露，导致用户和企业的利益严重受损。

1. 敏感信息泄露，大型企业商业机密堪忧

今年年初，“泄密门”事件持续升温，1 月 4 日晚，新浪爱问存在 SQL 注入漏洞，大约 7000 万明文存储的密码外泄。报告这个漏洞的白帽黑客(专业安全人员，非恶意黑客)对著名魔术师刘谦的微博进行了尝试性攻击，并取得成功。

4 月 25 日，国内知名的 PHP 应用程序织梦内容管理系统被发现其官方网站提供下载的织梦 CMS(Dedecms)v5.7 sp1 版本的中的 shopcar.class.php 文件被植入一句后门代码。通过利用这个后门，黑客只需要构造简单的数据包提交到服务器，就能够获取到该网站的 WebShell，通过对服务器进一步渗透攻击，进而获取服务器的最高权限，从而获取数据库中的所有信息。

从 CSDN 数据库泄露事件开始，敏感信息及数据库泄露事件就被更多的网民所熟知，同时，由于经济利益的驱使，黑客会尝试获取更多的数据库及相关数据。一时间，敏感信息泄露，威胁着许多大型企业的商业机密安全。许多大片中神奇的黑客技术如今已不是科幻，企业的核心技术、客户资料一旦被黑客盗取、贩售、公布，企业将面临前所未有的巨大危机。

2. 电子商务网站频遭攻击，用户经济利益遭受严重威胁

近日，一些主流的 B2C 网站正频频遭遇账户泄露、线上欺诈。

今年 3 月，著名电子商务网站当当网账户出现异常，超过 100 位用户账户里的钱被盗用或划走。3 月 19 日至 22 日，当当网被迫冻结了全部用户账户余额和礼品卡，对异常账户

进行清理。3 月 23 日解冻之后，当当网宣布对用户损失全额赔付。

6 月 24 日，京东商城的公告中爆出京东的一些用户 ID 被盗，目前，网站已采取更改密码、验证邮箱及开通手机提醒、支付密码等措施，提醒用户保护个人信息。

B2C 网站，作为电子商务零售企业，有义务保障自己用户的信息安全。然而，一连串的电商账号泄露事件，却让人不得不为 B2C 的账号安全担忧。很明显，目前我国的电商对信息安全不够重视，保障准备不足，才会出现如此大面积、持续的恶性事件。

3. 企业级、国家级信息对抗已升级至“核战”等级

1)超级病毒 Win32.Virut 持续在企业内活跃

在上半年中，瑞星“云安全”系统监测到一个名为 Win32.Virut 的病毒在国内企业中不断蔓延。该病毒感染性、粘滞性极强，已经成为了企业内部难以根治的顽疾。用户中毒后进程内会有异常的 EXPLORER.EXE 和 wsctf.exe，并会感染其他 exe 文件，也可能会后台下载其他病毒或木马，进而危害整个企业网络。

目前，瑞星杀毒软件网络版专门推出了针对 Win32.Virut 的防御方案，可以帮助企业有效的解决 Win32.Virut 病毒问题。

2)APT 攻击来临，网络“核战”爆发

APT 的直接翻译为“高级持续性攻击”，简单地讲，就是针对企业、研究机构或政府单位的不间断渗透，利用软硬件漏洞加社会工程学原理进行的持续攻击。商业竞争或经济利益带来的 APT 攻击事件越来越多，瑞星安全专家形象的将 APT 攻击比喻为网络时代的“核战”。毫不夸张的说，网络信息安全未来将成为影响企业生死存亡的关键性因素。

A.超级火焰病毒爆发

5 月 30 日晚，瑞星公司向全体网民发布红色安全警报：席卷全球的"超级火焰"病毒已

入侵我国，并大面积爆发。

该病毒非常复杂，危害性极高，一旦企业感染，将迅速蔓延至整个网络。病毒进入系统后，会释放黑客后门程序，利用键盘记录、屏幕截屏、录音、读取硬盘信息、网络共享、无线网络、USB 设备及系统进程等多种方式在被感染电脑上收集敏感信息，并发送给病毒作者，给用户造成巨大安全隐患。

同时，该病毒结构相当庞大，可以比喻成一个完整的“应用程序”，病毒包的完整大小有数十兆之多，其复杂性和危害性都大大超乎了用户对于一般病毒的理解。该病毒由多个功能模块构成，使用了至少 5 种加密算法、3 种压缩算法、5 种文件格式，并采用了特殊的代码注入技术，利用了大量系统漏洞进行入侵。

5 月 31 日，瑞星宣布针对席卷全球的“超级火焰”病毒已能提供解决方案，专杀工具已经上线，免费向全体用户开放。同时，瑞星公司已对全线产品进行了紧急升级，企业级用户已能够通过瑞星杀毒软件网络版拦截并彻底查杀此病毒。

B. 计算机病毒或成为国家武器

从“震网”到“火焰”，计算机病毒已经开始明显地服务于政治目的，并在国家对抗中崭露头角。目前，中东地区在这几年成为超级蠕虫的主要攻击目标，这与国际时事环境是密切不可分的。

因此，在这样的国际局势下，基础软件的自主产权显得越来越重要，尤其是关键的工业、军事领域中的工业控制、信息安全等基础软件，将成为国家安全机制中的重要一环。

4. 大型攻击针对银行、支付领域

据法国媒体 6 月 28 日报道，美国一份保安报告显示，最近有不法分子对银行发动一轮网络攻击，欧美及其他地区的多个银行户头已被盗取至少 8000 万美元（约合人民币 5 亿元）。诈骗集团攻击了全球至少 60 家银行的网络，他们利用自动化等尖端技术，专门向拥有巨额存款的账户下手。

国内的金融信息安全状况也令人堪忧！今年 2 月 21 日，国内知名银行的 ATM（网银自助服务机）就曾发现安全漏洞，可被黑客利用来侵入银行内网，套取用户资料和金钱等。“类似 ATM 这样关系到人民财产安全的重要设施一旦成为黑客攻击的对象，后果不堪设想，并且用户很难获得赔偿”，瑞星安全专家指出。以往被人们相信很安全的银行，尤其是国际的大银行也出现了严重安全问题，足见黑客之猖獗。

“黑客的攻击行为表现出了日益增强的自动化程度和复杂性。在某些案件中，攻击者不用积极参与就能掌控受害者的账户。”瑞星安全专家指出，在某些案件中，犯罪分子能够规避很多欧洲银行用以进行额外身份认证的智能卡读卡器。黑客一旦入侵银行系统就有可能窃取银行卡账号密码、进行转账等操作，广大用户应注意安全。广大企业尤其是银行金融业，要提高安全意识，切实保障用户账号安全。

五、下半年信息安全趋势展望

1.移动互联网危机四伏

移动互联网将成为黑客下半年攻击的重点，从技术上分析，已经可以看出，手机病毒将通过利用系统底层技术实现更复杂的恶意行为。从环境上分析，无线公共网络在方便了用户的同时，也存在着巨大的隐私泄露威胁。

可以看出，移动互联网安全从一开始就带有时代的烙印。无论是恶意扣费，还是银行账号盗窃，这些恶意行为的背后，几乎全部带有经济利益指向性。

很快，移动互联网将出现传统互联网的症状，针对移动互联网的挂马、网络钓鱼，相信也会出现在不久的将来。无论是企业还是个人，都应对此予以警惕，提早做好安全防护工作，以避免未来可能出现的损失。

2.个人隐私安全堪忧

个人隐私泄露的威胁已经让全社会警醒，而黑客也在其中捞足了好处。预计下半年，不法分子还将继续设法窃取用户的隐私信息。病毒、挂马网站、钓鱼网站等针对个人隐私信息的大规模攻击仍不可避免，企业和个人应采取积极的态度防御应对。

3.针对企业级、国家级的网络攻击或将大规模爆发

“超级火焰”病毒虽然已在我国被成功拦截，但是在世界上许多国家和地区，还仍然横行肆虐。这种针对企业级、国家级的网络攻击在未来还将持续很长一段时间。“超级火焰”显然不是第一个，更不会是最后一个。

规模更大、技术更先进的大型网络攻击，在今后有可能演变为“核战”级企业、国家之间的科技与信息对抗。由此可见，自主研发的信息安全技术在现代网络战争中已经处于越来越重要的位置。