2018 年上半年中国网络安全报告

北京瑞星网安技术股份有限公司

2018 年 7 月

免责声明

本报告综合瑞星“云安全”系统、瑞星安全研究院、瑞星威胁情报平台、瑞星客户服务中心等部门的统计、研究数据和分析资料，针对中国 2018 年 1 至 6 月的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网络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

报告摘要

- 2018 年上半年瑞星“云安全”系统共截获病毒样本总量 2,587 万个，病毒感染次数 7.82 亿次。北京市病毒感染 1.93 亿人次，位列全国第一，其次为广东省 0.57 亿人次。

- 2018 年上半年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 4,785 万个，其中挂马网站 2,900 万个，诈骗网站 1,885 万个。美国恶意 URL 总量为 1,643 万个，位列全球第一，其次是中国 226 万个，德国 72 万个，分别为二、三位。

- 2018 年上半年瑞星“云安全”系统共截获手机病毒样本 345 万个，新增病毒类型以信息窃取、资费消耗四类为主，其中信息窃取类病毒占比 28%，位居第一。其次是资费消耗类病毒占比 27%，第三名是流氓行为类病毒，占比 17%。

- 2018 年上半年移动安全事件：“旅行青蛙”游戏外挂藏风险；恶意软件伪装“系统 Wi-Fi 服务”感染近五百万台安卓手机；二手手机信息泄露乱象：10 元可买通讯录，几十元可恢复已经删除的数据。

- 2018 年上半年全球网络安全事件解读：英特尔处理器曝“Meltdown”和“Spectre 漏洞”；湖北某医院内网遭到挖矿病毒疯狂攻击；中国某军工企业被美、俄两国黑客攻击；Facebook 用户数据泄露；GitHub 遭受有史以来最严重 DDoS 攻击；A 站受黑客攻击 近千万条用户数据外泄。

- 2018 年上半年流行病毒分析：MsraMiner 挖矿病毒；蠕虫化的勒索病毒；VPNFilter 物联网病毒；网页挖矿病毒新变化。

- 趋势展望：犯罪团伙转向挖矿与勒索；漏洞利用越来越广泛；物联网病毒更加精密。

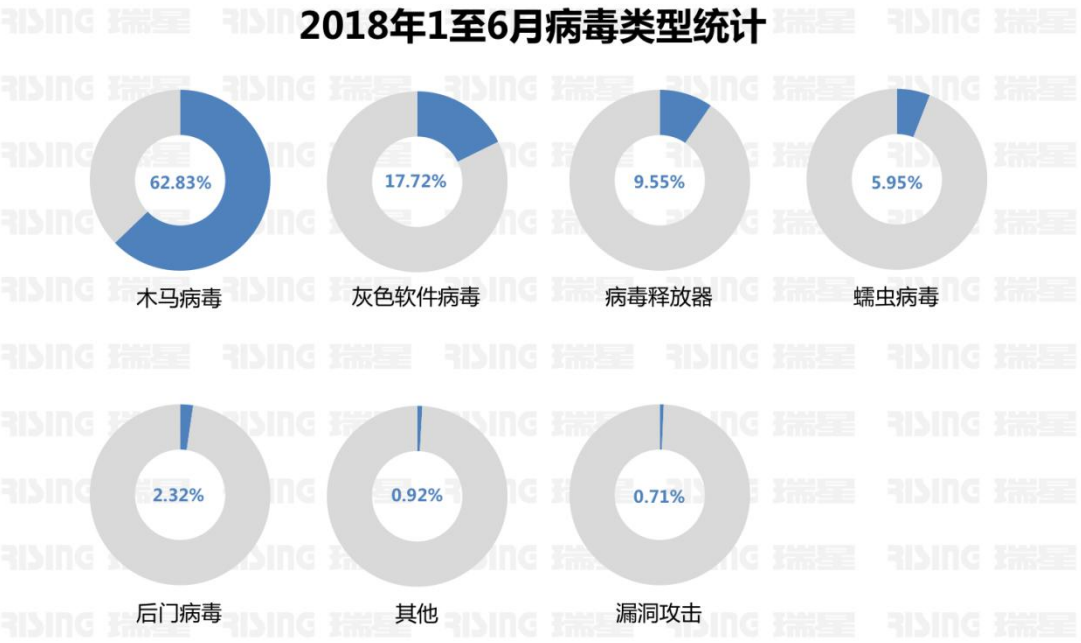
一、恶意软件与恶意网址

（一）恶意软件

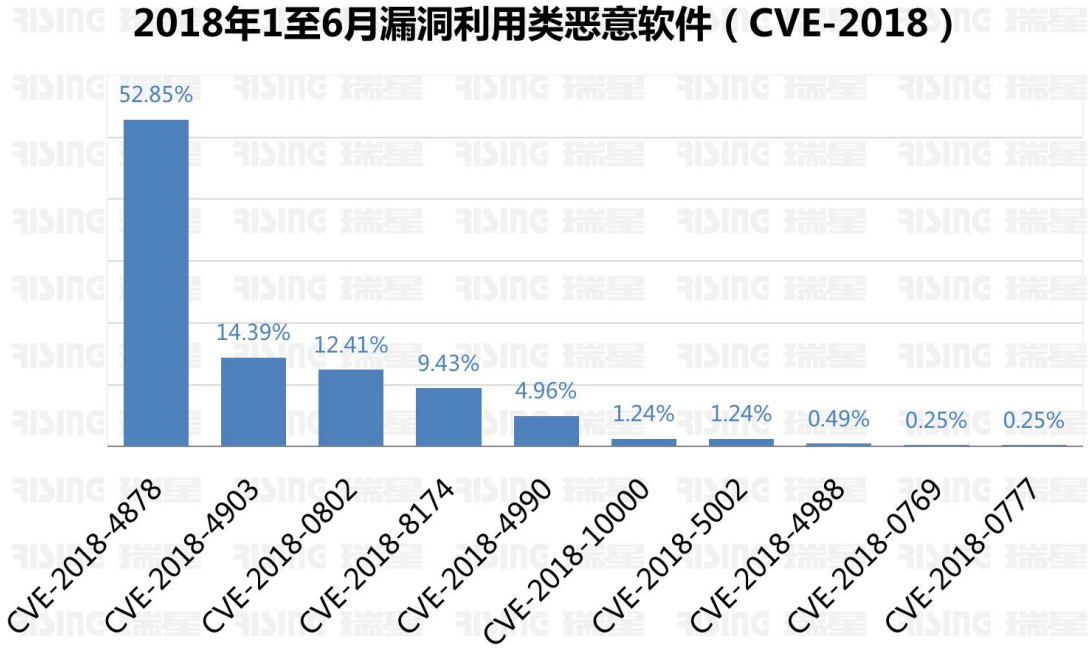
1. 2018 年上半年病毒概述

（1）病毒疫情总体概述

2018 年上半年瑞星“云安全”系统共截获病毒样本总量 2,587 万个，病毒感染次数 7.82 亿次。新增木马病毒占总体数量的 62.83%，依然是第一大种类病毒。灰色软件病毒（垃圾软件、广告软件、黑客工具、恶意软件）为第二大种类病毒，占总体数量的 17.72%，第三大种类病毒为病毒释放器，占总体数量的 9.55%。



报告期内，CVE-2018-4878 漏洞利用占比 52.85%，位列第一位。该漏洞影响 Flash Player 所有版本，攻击者可以诱导用户打开包含恶意 Flash 代码文件的 Microsoft Office 文档、网页、垃圾电子邮件等。



（2）病毒感染地域分析

报告期内，北京市病毒感染 1.93 亿人次，位列全国第一，其次为广东省 0.57 亿人次及山东省 0.44 亿人次。

2. 2018 年上半年病毒 Top10

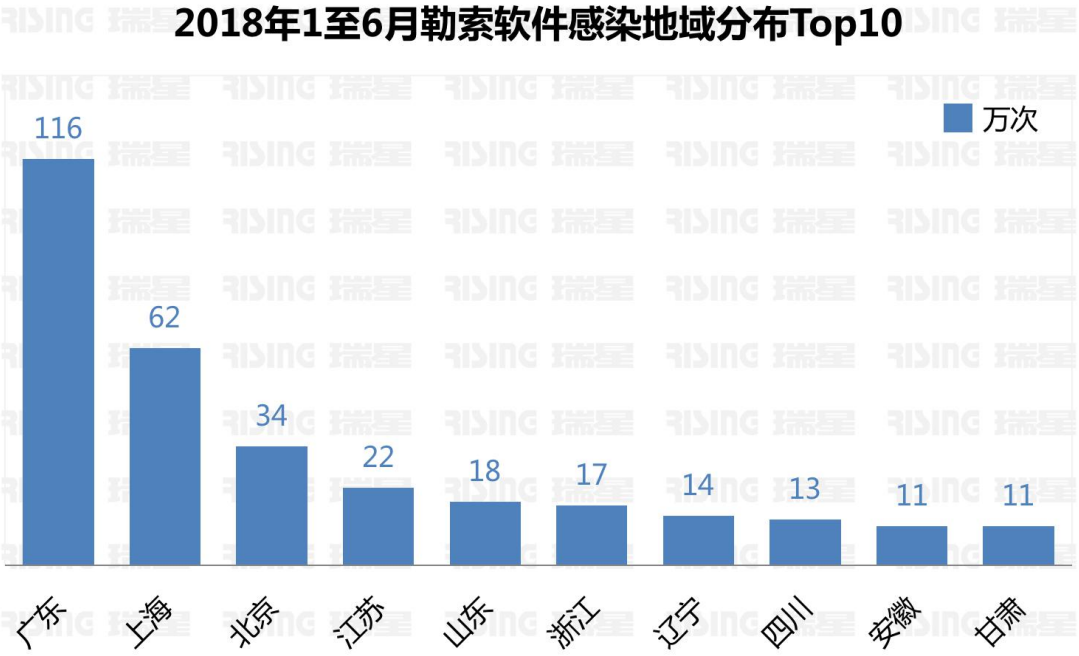
根据病毒感染人数、变种数量和代表性进行综合评估，瑞星评选出了 2018 年上半年 1 至 6 月病毒 Top10：

2018年1至6月病毒Top10

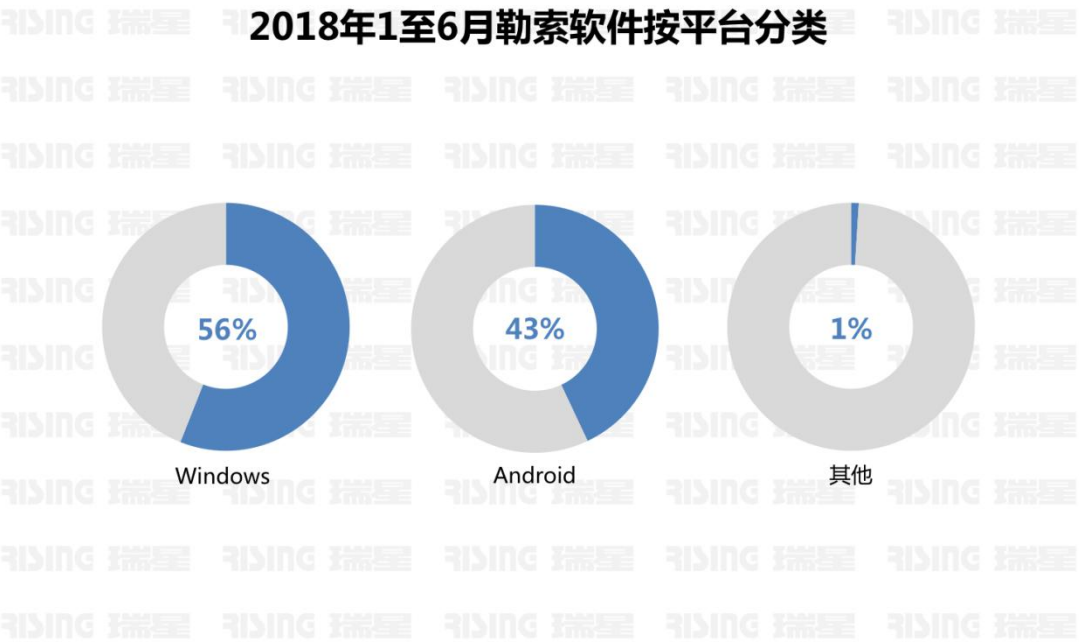
1	Trojan.Vools!8.F279	通过漏洞传播，窃取敏感信息的木马病毒
2	Backdoor.Agent!8.C5D	使用永恒之蓝攻击工具包，攻击局域网中的计算机，传播挖矿病毒
3	Trojan.TaojinStar!8.B91	窃取敏感信息的木马病毒
4	Trojan.Win32/64.XMR-Miner!1.ADCC	挖矿木马
5	Trojan.ShadowBrokers!8.B976	漏洞利用木马病毒
6	Trojan.Agent!8.B1E	具有常见木马行为的一类病毒
7	Trojan.CoinMiner!8.30A	挖矿木马
8	Trojan.Reconyc!8.153	伪装系统程序，加载病毒模块
9	Downloader.Chindo!8.436	从网络上下载其他木马病毒
10	Dropper.Generic!8.35E	病毒释放器，执行后释放病毒文件

3. 2018 年上半年中国勒索软件感染现状

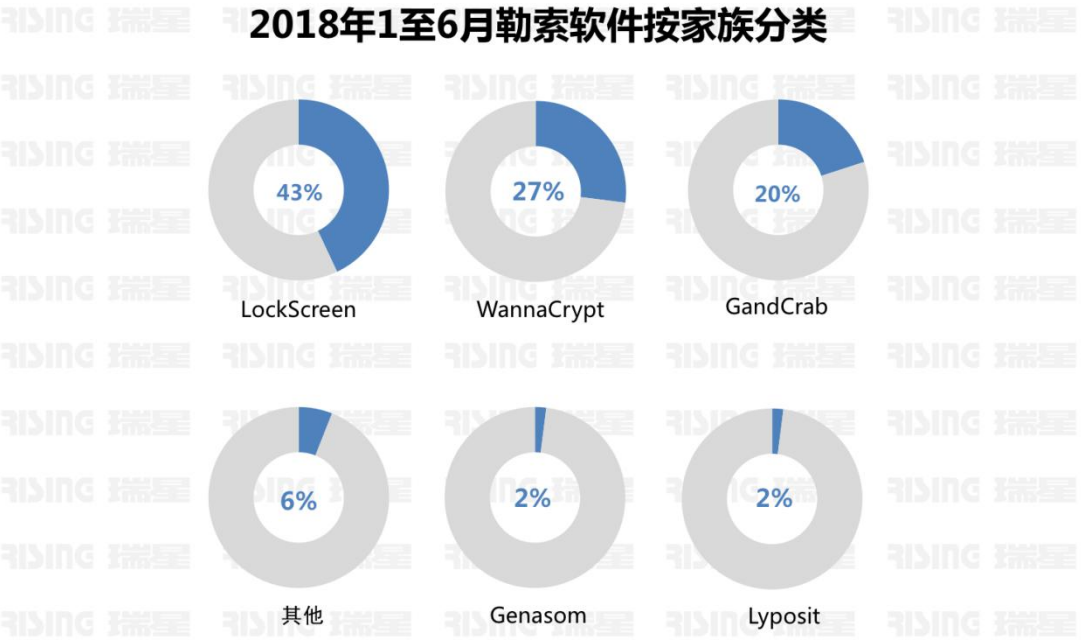
报告期内，瑞星“云安全”系统共截获勒索软件样本 31.44 万个，感染共计 456 万次，其中广东省感染 116 万次，位列全国第一，其次为上海市 62 万次，北京市 34 万次及江苏省 22 万次。



通过对瑞星捕获的勒索样本按平台分析发现，Windows 平台占比 56%，Android 平台占比 43%。



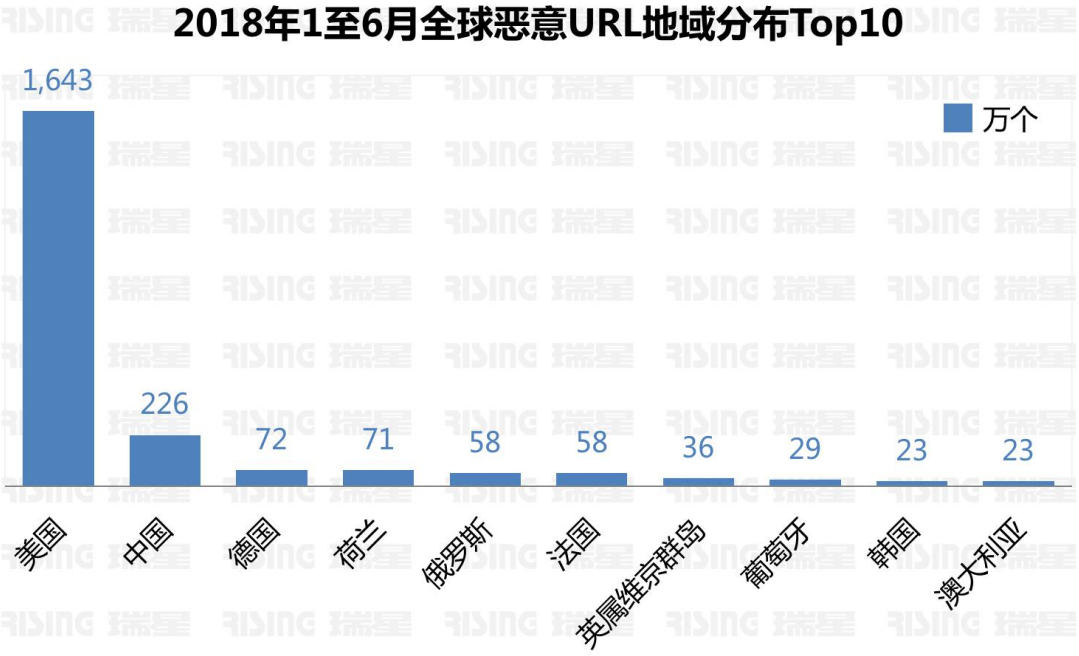
通过对瑞星捕获的勒索样本按家族分析发现，LockScreen 家族占比 43%，位列第一，其次为 WannaCrypt 占比 27%，以及 GandCrab 占比 20%。



（二）恶意网址

1. 2018 年上半年全球恶意网址总体概述

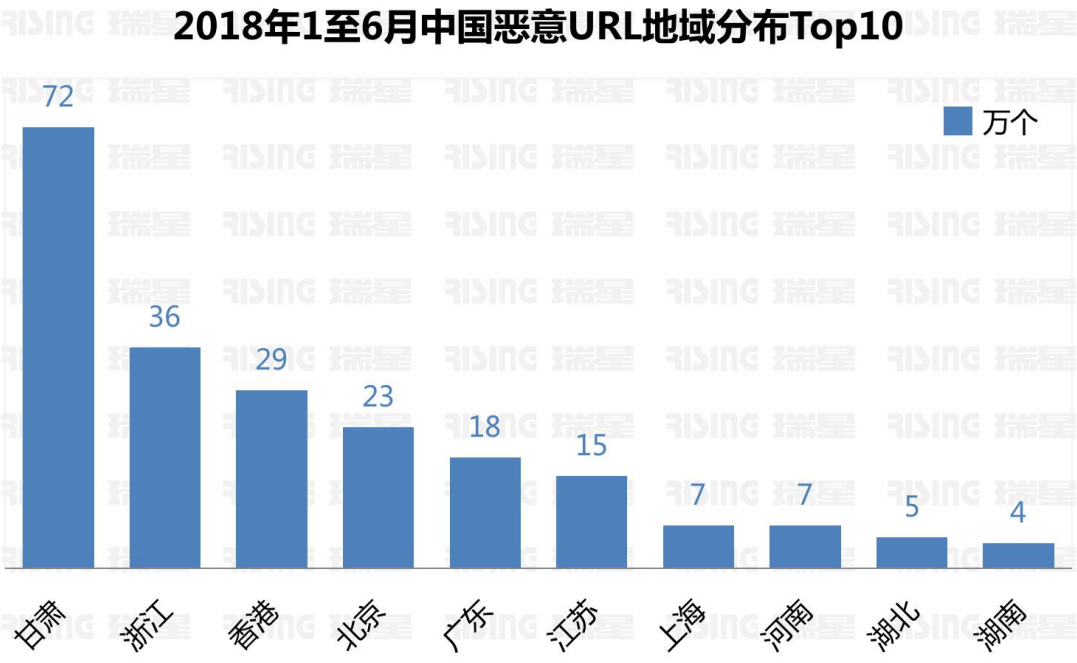
2018 年上半年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 4,785 万个，其中挂马网站 2,900 万个，诈骗网站 1,885 万个。美国恶意 URL 总量为 1,643 万个，位列全球第一，其次是中国 226 万个，德国 72 万个，分别为二、三位。



2. 2018 年上半年中国恶意网址总体概述

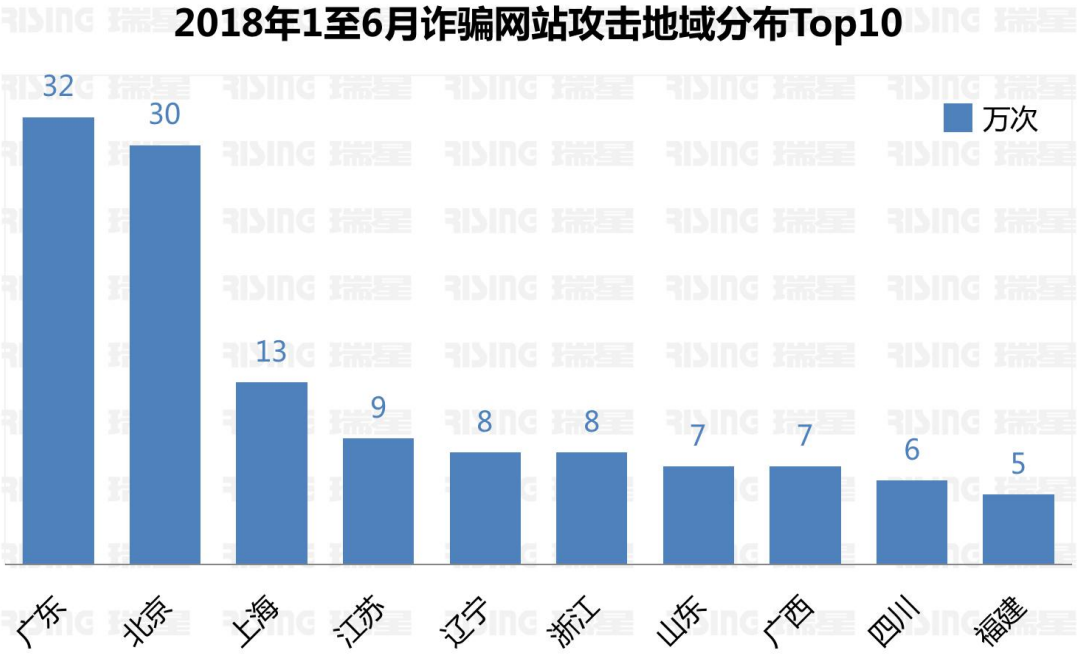
报告期内，甘肃省恶意网址（URL）总量为 72 万个，位列全国第一，其次是浙江省 36 万个，以及香港 29 万个，分别为二、三位。

注：上述恶意 URL 地址为恶意 URL 服务器的物理地址。

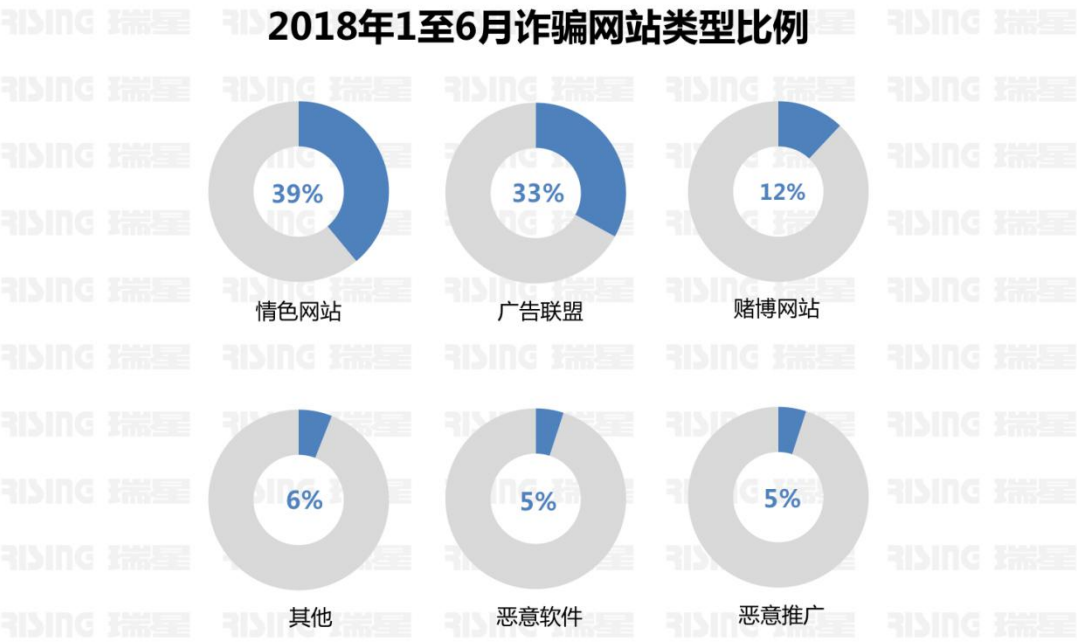


3. 2018 年上半年中国诈骗网站概述

2018 年上半年瑞星“云安全”系统共拦截诈骗网站攻击 182 万余次，广东受诈骗网站攻击 32 万次，位列第一位，其次是北京市受诈骗网站攻击 30 万次，第三名是上海市受诈骗网站攻击 13 万次。



报告期内，情色类诈骗网站占 39%，位列第一位，其次是广告联盟类诈骗网站占 33%，赌博类诈骗网站占 12%，分别为二、三位。



4. 2018 年上半年中国主要省市访问诈骗网站类型

报告期内，北京、辽宁、浙江等地区访问的诈骗网站类型以情色网站为主，广东、山东、广西等地区则以在线赌博为主，其余地区访问恶意推广诈骗网站居多。

2018年1至6月中国主要省市访问诈骗网站类型

地区	类型
广东	赌博
北京	情色
上海	恶意推广
江苏	恶意推广
辽宁	情色
浙江	情色
山东	赌博
广西	赌博
四川	情色
福建	赌博

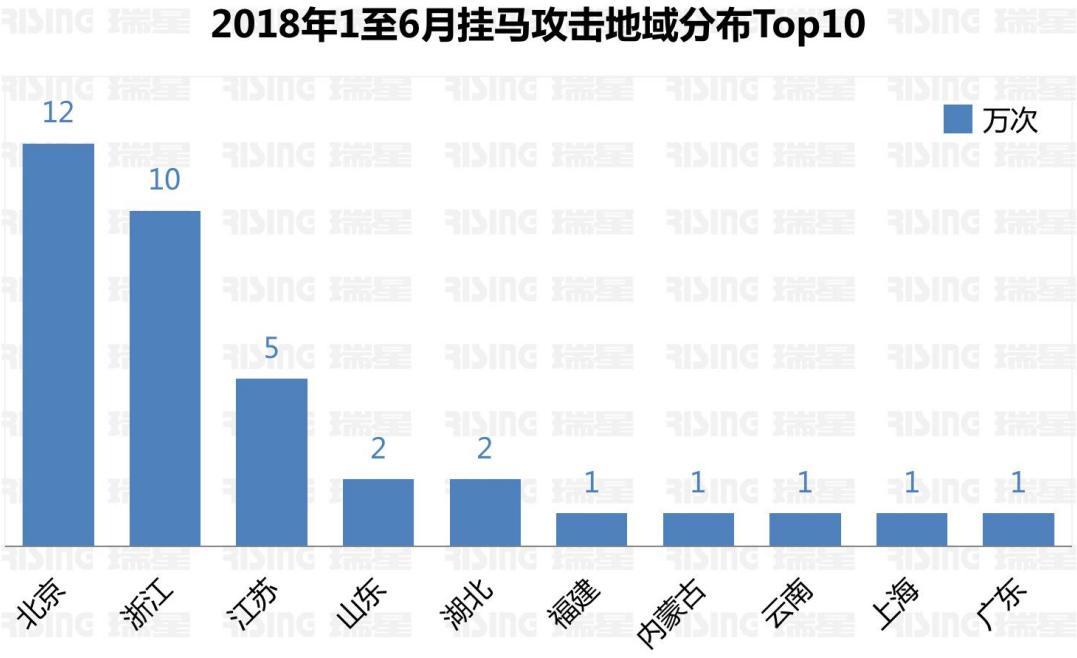
5. 诈骗网站趋势分析

2018 年上半年情色、赌博类诈骗网站占比较多，这些恶意网站大多通过非法手段进行传播，赌博类诈骗网站利用高利润的方式吸引用户，前期平台方会在后台操作让用户少输多赢，当用户产生一定的兴趣后，再进行后台操作赢取用户钱财。诈骗网站的传播途径：

- 利用微信朋友圈以软文方式进行诱导传播。
- 利用 QQ 群发方式进行范围传播。
- 利用短信群发平台以中奖方式进行传播。
- 利用游戏辅助软件进行传播。
- 利用大型互联网平台发布信息进行传播。

6. 2018 年上半年中国挂马网站概述

2018 年上半年瑞星“云安全”系统共拦截挂马网站攻击 38 万余次，北京市受挂马攻击 12 万次，位列第一位，其次是浙江省受挂马攻击 10 万次。



7. 挂马网站趋势分析

2018 年上半年挂马攻击相对减少，攻击者一般自建一些导航类或色情类网站，吸引用户主动访问。有些网站会锁定用户浏览器主页，当用户访问会自动跳转到指定的恶意网站，大部分恶意网站会挂载木马程序诱导用户下载，进而窃取用户的账户信息，非法分子利用窃取的信息进行诈骗或资金盗刷。挂马防护手段主要为：

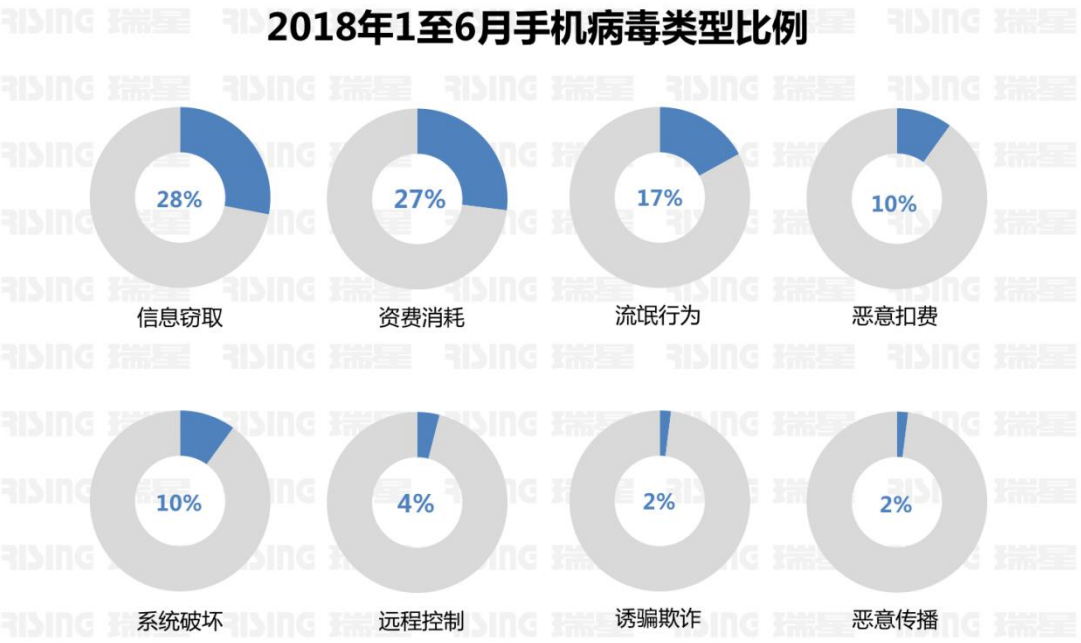
- 更新到最新的浏览器版本。
- 禁止浏览陌生邮件或手机短信发送的链接网址。
- 禁止浏览不正规或非法网站。
- 禁止在非正规网站下载软件程序。
- 安装杀毒防护软件。

二、移动互联网安全

（一）手机安全

1.2018 年上半年手机病毒概述

2018 年上半年瑞星“云安全”系统共截获手机病毒样本 345 万个，新增病毒类型以信息窃取、资费消耗四类为主，其中信息窃取类病毒占比 28%，位居第一。其次是资费消耗类病毒占比 27%，第三名是流氓行为类病毒，占比 17%。



2.2018 年上半年手机病毒 Top5

2018年1至6月手机病毒Top5

序号	病毒名	恶意行为
1	Trojan.SMSreg!8.2DFC	发送扣费短信，窃取用户短信收件箱、通讯录等行为。
2	Dropper.Shedun/Android!8.3F4	私自拨打电话，私发短信、彩信、邮件，频繁连接网络，窃取用户短信收件箱等行为。
3	Dropper.Agent/Android!8.37E	通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱导用户触发点击等行为。
4	Trojan.SMSSend!8.2DF7	启动后拦截用户短信，并将短信转发给指定号码，泄漏短信中的账户或密码,并上传手机联系人信息、收发件箱、通讯录、来电号码至指定服务器。
5	Trojan.Hiddad/Android!8.4E1	伪装成合法程序，推送广告，消耗用户流量，窃取用户隐私数据。

3. 2018 年上半年 Android 手机漏洞 Top5

2018年1至6月Android手机漏洞Top5

序号	漏洞名称	漏洞编号	简介
1	RAMpage漏洞	CVE-2018-9442	Android设备存在RAMpage漏洞。攻击者可以在设备上运行的非特权Android应用程序。
2	Qualcomm 组件权限提升漏洞	CVE-2018-5835	Android Qualcomm组件WLAN Host存在权限提升漏洞。攻击者可利用该漏洞实现权限提升。
3	Framework架构权限提升漏洞	CVE-2018-9433	远程攻击者使用经过特殊处理的PAC文件在特权进程的上下文中执行任意代码。
4	Media架构组件权限提升漏洞	CVE-2018-9411	这漏洞会让远程攻击者可透过特制文件档案获得授权，同时也能执行任何程式码。
5	System系统漏洞	CVE-2018-9365	影响 Kernel 的最严重漏洞，该漏洞可能被远程攻击者利用执行任意代码。

（二）2018 年上半年移动安全事件

1.“旅行青蛙”游戏外挂藏风险

2018 年 1 月，一款名为“旅行青蛙”的手游在朋友圈中刷屏。因为操作简单、节奏缓慢，这款游戏也被网友戏称为“佛系养蛙”。部分商家瞅准商机，针对 iOS 手机用户，推出“花费 20 元即可购买 21 亿无限三叶草”服务，通过“外挂”操作，让玩家轻易获得大量三叶草。记者调查发现，购买“无限三叶草”服务后，需要在电脑上按照教程操作或允许商家远程操作，但其间存在不少风险，或会造成手机中数据丢失，甚至泄露个人隐私。

2.恶意软件伪装“系统 Wi-Fi 服务”感染近五百万台安卓手机

2018 年 3 月，安全研究人员发现一个大规模持续增长的恶意软件活动，已经感染了全球近 500 万台移动设备。一款名为“Rottensys”的恶意软件伪装成“系统 Wi-Fi 服务”，该程序包含风险代码，可在后台私自下载恶意插件并静默安装，进行远程控制命令以及对用户手机进行 root，从而频繁推送广告并进行应用分发，消耗用户流量资费，影响用户体验。受影响的品牌包括荣耀、华为、小米、OPPO、Vivo、三星和金力等。

3.二手手机信息泄露乱象：10 元可买通讯录，几十元可恢复已经删除的数据

2018 年 6 月，有记者调查发现，网上有收售二手手机、电脑的贩子以一毛钱一条的价格打包出售机主信息。而在二手手机交易和手机维修市场中，很多维修商称只需花几十元就能恢复手机通讯录、照片、微信聊天记录等，哪怕手机被恢复到出厂设置，也可以将删除的信息复原。专家表示，要想手机信息不被泄露，通常需要从硬件安全和软件安全两方面去解决。“硬件安全就是外界所说的用水泡或者将手机砸烂。但这种方式无论从环保性还是经济性而言，成本太高。”软件安全，则是用户为了规避隐私风险，在出售手机前可以通过第三方粉碎软件将所有个人信息删除粉碎，同时需要解除手机上涉及网络支付的所有软件绑定。

三、互联网安全

（一）2018 年上半年全球网络安全事件解读

1.英特尔处理器曝“Meltdown”和“Spectre 漏洞”

2018 年 1 月，英特尔处理器中曝“Meltdown”（熔断）和“Spectre” （幽灵）两大新型漏洞，包括 AMD、ARM、英特尔系统和处理器在内，几乎近 20 年发售的所有设备都受到影响，受影响的设备包括手机、电脑、服务器以及云计算产品。这些漏洞允许恶意程序从其它程序的内存空间中窃取信息，这意味着包括密码、帐户信息、加密密钥乃至其它一切在理论上可存储于内存中的信息均可能因此外泄。

2.湖北某医院内网遭到挖矿病毒疯狂攻击

2018 年 3 月，湖北某医院内网遭到挖矿病毒疯狂攻击，导致该医院大量的自助挂号、缴费、报告查询打印等设备无法正常工作。由于这些终端为自助设备，只提供特定的功能，安全性没有得到重视，系统中没有安装防病毒产品，系统补丁没有及时更新，同时该医院中各个科室的网段没有很好的隔离，导致挖矿病毒集中爆发。

3.中国某军工企业被美、俄两国黑客攻击

2018 年 3 月，安全研究人员表示，中国某军工企业被美、俄两国黑客攻击。美国黑客和俄罗斯黑客在 2017 年冬天入侵了中国一家航空航天军事企业的服务器，并且留下了网络

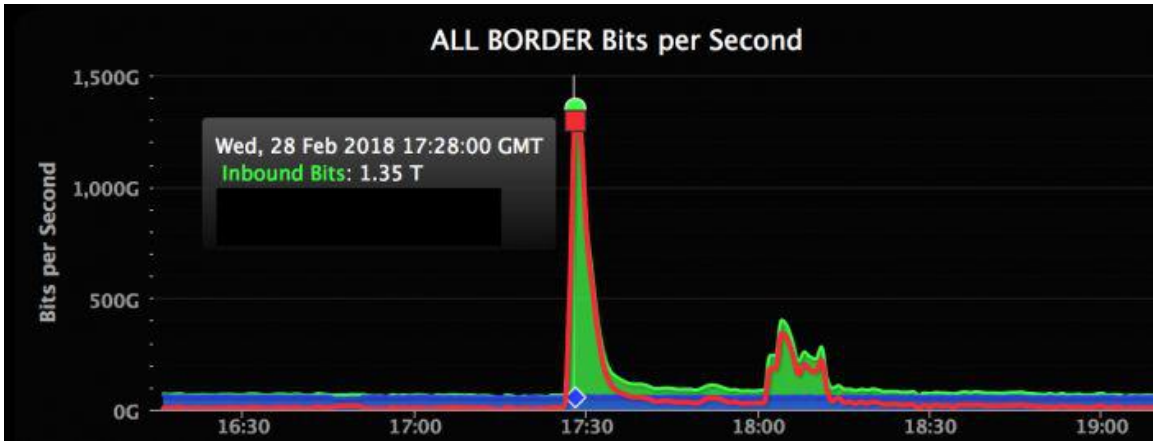
间谍工具。研究人员认为这种情况比较罕见，以前从未发现俄罗斯黑客组织 APT28 与美国 CIA 的黑客组织 Lamberts （又被称为“长角牛”Longhorn）攻击同一个系统。

4.Facebook 用户数据泄露

2018 年 3 月，Facebook 八千七百多万用户数据泄露，这些数据被“剑桥分析”公司非法利用以发送政治广告。此次事件被视为 Facebook 有史以来遭遇的最大型数据泄露事件。剑桥分析公司与 Facebook 进行了合作。前者开发了一个让用户进行“个性人格测试”的 Facebook App（类似国内微信的小程序），每个用户做完这个测试，就可以得到 5 美元。剑桥分析公司不仅收集了用户的测试结果，顺便收集了用户在 Facebook 上的个人信息。剑桥分析公司以此访问并获得了 8700 万活跃用户数据，然后建立起用户画像，依靠算法，根据每个用户的日常喜好、性格特点、行为特征，预测他们的政治倾向，然后定向向用户推送新闻，借助 Facebook 的广告投放系统，影响用户的投票行为。

5.GitHub 遭受有史以来最严重 DDoS 攻击

2018 年 3 月，知名代码托管网站 GitHub 遭遇了有史以来最严重的 DDoS 网络攻击，峰值流量达到了 1.35Tbps。尽管此类攻击的特点就是利用如潮水般的流量同时涌入网站，不过本次攻击不同之处在于采用了更先进的放大技术，目的是针对主机服务器产生更严重的影响。这项新技术并非依赖于传统的僵尸网络，而是使用了 memcached 服务器。该服务器的设计初衷是提升内部网络的访问速度，而且应该是不暴露在互联网中的。不过根据 DDoS 防御服务提供商 Akamai 的调查，至少有超过 5 万台此类服务器连接到互联网上，因此非常容易受到攻击。



6.A 站受黑客攻击 近千万条用户数据外泄

2018 年 6 月，弹幕视频网 AcFun 公告称，因网站受黑客攻击，已有近千万条用户数据外泄，目前已报警处理，希望用户及时修改密码。公告称，用户数据泄露的数量达近千万条，原因是遭到黑客攻击。泄露的数据主要包括用户 ID、昵称、加密储存的密码等。A 站表示，本次事件的根本原因在于公司没有把 AcFun 做得足够安全，为此，官方向用户道歉，并将马上提升用户数据安全保障能力。目前，A 站已联合内部和外部的技术专家成立了安全专项组，排查问题并升级了系统安全等级。此后，公司将对 AcFun 服务做全面系统加固，实现技术架构和安全体系的升级。

（二）2018 年上半年流行病毒分析

1.MsraMiner 挖矿病毒

2018 年最大的变化是病毒制造者将目标投向了挖矿领域，大量的挖矿病毒层出不穷，其中影响最大的是一个构造精密被称为 “MsraMiner”的挖矿僵尸网络。此病毒利用永恒之蓝漏洞攻击局域网中的机器，中毒机器会继续使用永恒之蓝漏洞攻击其它机器，并作为 web 服务器供其它机器下载，导致大量局域网主机被植入挖矿病毒，同时病毒持续升级对抗查杀。导致此病毒爆发的主要原因是：

（1）企业存在大量机器没有安装永恒之蓝漏洞补丁。
（2）企业内外网混用，并没有做到真正的隔离，连接互联网的一台机器中毒后，导致公司内网机器大量中毒。
（3）企业没有安装杀毒软件，没有及时更新病毒库，为病毒传播制造了有利条件。

2、蠕虫化的勒索病毒

从 WannaCry 勒索病毒爆发以来，勒索病毒层出不穷，并且勒索病毒蠕虫化变得更加流行起来。2018 年 2 月份，两家省级医院感染勒索病毒，导致服务中断。感染原因被怀疑是系统存在漏洞和弱口令，导致攻击者植入勒索病毒，并快速传播。

其中影响较大的 Satan 勒索病毒，不仅使用了永恒之蓝漏洞传播，还内置了多种 web 漏洞的攻击功能。相比传统的勒索病毒传播速度更快。虽然已经被解密，但是此病毒利用的传播手法却非常危险。

3、VPNFilter 物联网病毒

VPNFilter 恶意软件是一个多阶段、模块化的平台，具有多种功能，可支持情报收集和破坏性网络攻击操作，可感染 71 款甚至更多物联网设备，这些设备包括路由器、摄像头、机顶盒等。物联网设备中毒后较难发现，漏洞难以及时修补，甚至有的设备已经找不到生产厂商。这些感染物联网病毒的僵尸设备，会对全球网络安全造成很大的隐患。

4、网页挖矿病毒新变化

全球将近 5 万家网站被攻击者植入挖矿脚本，其中很大一部分是 Coinhive 脚本。Coinhive 专门提供一个用来挖矿的 JS 引擎，当用户访问含有 Coinhive 代码的网页时，Coinhive 的 JS 代码库就会在用户的浏览器上运行，挖矿程序就会开始工作，挖掘门罗币，消耗用户计算机的 CPU 资源。使用 Coinhive 默认的方式挖矿，已经很容易被发现。2018 年上半年，网页挖矿病毒又出现新变化，出现了两种新的攻击方式，一种是做一个中转再访问 Coinhive 挖矿脚本的链接，另一种是自建平台不使用 Coinhive，这种方式更加隐蔽，并且避免了 Coinhive 平台的手续费。

四、趋势展望

（一）犯罪团伙转向挖矿与勒索

近年来，挖矿和勒索病毒持续上升，传统 DDOS 和刷流量的病毒仍然存在，但有一定的下降，一方面 DDOS 和刷流量的病毒过于显眼，另一方面相关部门加大了打击力度。虚拟货币的钱包地址比较隐蔽，一般情况下很难通过钱包地址定位到攻击者的身份。无论是加密货币挖矿的钱包地址，还是勒索病毒索要赎金的钱包地址都是虚拟货币钱包，因此催生了加密货币挖矿病毒和勒索病毒的爆发。

（二）漏洞利用越来越广泛

以前漏洞大部分都是 APT 团伙在使用，但随着经济利益的驱使，挖矿和勒索病毒也开始使用漏洞，而且使用漏洞的种类开始增加，这就导致很多受害者，并没有下载运行可疑程序也有可能中毒。尤其是服务器，运行了很多 web 服务、数据库服务、开源 CMS 等服务，这些服务经常会出现漏洞，如果服务器没有及时更新补丁，就会被攻击者通过漏洞植入病毒，而且很多公司的外网服务器和内网是连通的，一旦服务器中毒，就可能导致局域网很多机器中毒。

（三）物联网病毒更加精密

物联网病毒最知名的是“Mirai”，它被用来发动 DDOS 攻击，后续基于“Mirai”修改而来的变种大多也是为了 DDOS 攻击。然而随着物联网设备的增多，物联网病毒也会有更多的功能，比如路由器中了病毒，就可能导致网络通信中的帐号密码等隐私信息被窃取。如果摄像头中了病毒，就可能导致一举一动都在攻击者的监控之中。如果中病毒的是工控设备，就可能导致工厂停产、城市停电等严重问题。

未来一段时间，利用漏洞攻击的挖矿和勒索病毒仍会持续增加，物联网病毒的数量和功能仍将持续增长。因此用户需要及时更新补丁，升级系统固件，安装防病毒产品，降低中毒的风险。