《2017 年中国网络安全报告》

本报告涵盖恶意软件与恶意网址、移动安全、互联网安全、趋势展望等多个章节，从解各方面分析 2017 中国网络安全态势。

一、恶意软件与恶意网址

（一）恶意软件

1. 2017 年病毒概述

（1）病毒疫情总体概述

2017 年瑞星“云安全”系统共截获病毒样本总量 5,003 万个，病毒感染次数 29.1 亿次，病毒总体数量比 2016 年同期上涨 15.62%。

报告期内，新增木马病毒占总体数量的 51.83%，依然是第一大种类病毒。蠕虫病毒为第二大种类病毒，占总体数量的 24.49%，第三大种类病毒为灰色软件病毒（垃圾软件、广告软件、黑客工具、恶意软件），占总体数量的 10.77%。

报告期内，CVE-2017-0147 漏洞利用占比 55%，位列第一位。该漏洞便是“永恒之蓝”漏洞，它是 2017 年泄露的 NSA 网络武器库中的一款攻击程序，其中利用了多个 Windows SMB 服务的零日漏洞。“永恒之蓝”威力巨大，利用此工具可以非常简单地入侵 Windows 系统。在今年 5 月，臭名昭著的勒索蠕虫 WannaCry 利用的便是“永恒之蓝”，从而造成了波及全球的破坏。

（2）病毒感染地域分析

报告期内，北京市病毒感染 3.01 亿人次，位列全国第一，其次为新疆省 2.49 亿人次及广东省 2.03 亿人次。

2. 2017 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 2017 年 1 至 6 月病毒 Top10：

2017年病毒Top10

1	Trojan.TaojinStar!8.B91	窃取敏感信息的木马病毒
2	Trojan.CoinMiner!8.30A	挖矿木马
3	Trojan.Inject!8.103	把自身注入到系统进程的木马病毒
4	Dropper.Generic!8.35E	病毒释放器，执行后释放病毒文件
5	Dropper.Dinwod!8.3BD	病毒释放器，执行后释放病毒文件
6	Trojan.PSW.Win32.Agent.exw	窃取账号的木马病毒
7	Worm.VobfusEx!1.99DF	伪装成文件夹、视频、图片等图标的蠕虫病毒
8	Trojan.Miner!8.EA1	挖矿木马
9	Trojan.WebHijack!8.2A51	浏览器劫持木马，重定向搜索请求，以显示未经请求的广告
10	Trojan.Kryptik!8.8	感染后可被黑客控制沦为“肉鸡”

3. 2017 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 92.99 万个，感染共计 1,346 万次，其中广东省感染 262 万次，位列全国第一，其次为上海市 159 万次，北京市 131 万次及江苏省 98 万次。

（二）恶意网址

1. 2017 年全球恶意网址总体概述

2017 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 8,011 万个，其中挂马网站 4,275 万个，诈骗网站 3,735 万个。美国恶意 URL 总量为 2,684 万个，位列全球第一，其次是中国 1,350 万个，韩国 507 万个，分别为二、三位。

2. 2017 年中国恶意网址总体概述

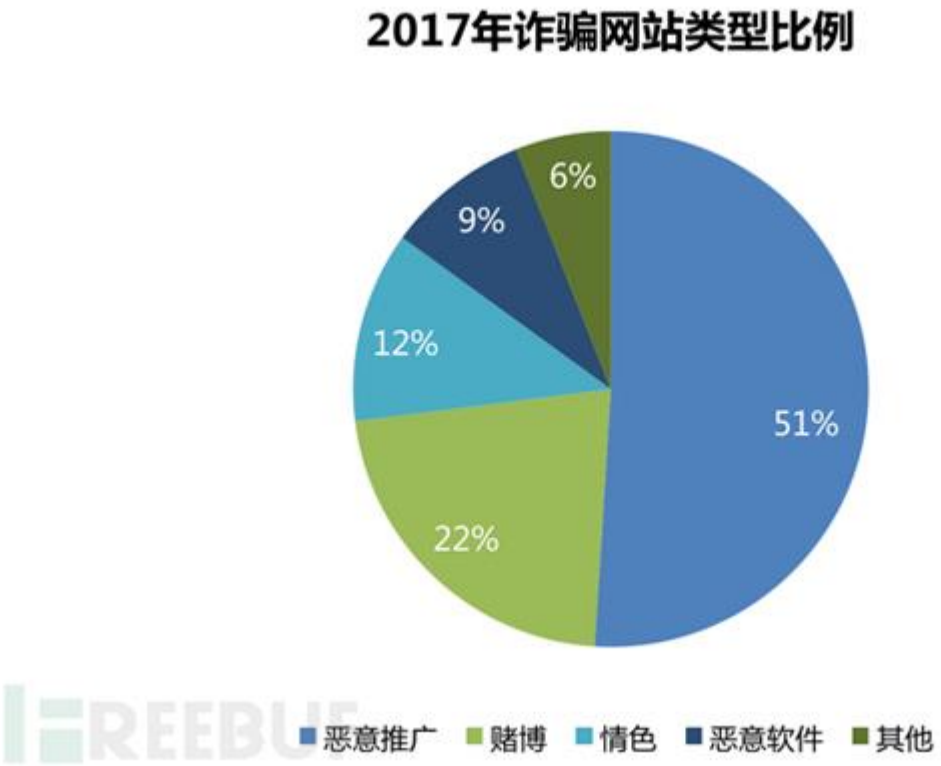
报告期内，北京市恶意网址（URL）总量为 558 万个，位列全国第一，其次是陕西省 233 万个，以及江苏省 100 万个，分别为二、三位。

注：上述恶意 URL 地址为恶意 URL 服务器的物理地址。

3. 2017 年中国诈骗网站概述

2017 年瑞星“云安全”系统共拦截诈骗网站攻击 740 万余次，广东受诈骗网站攻击 97 万次，位列第一位，其次是北京市受诈骗网站攻击 92 万次，第三名是浙江省受诈骗网站攻击 75 万次。

报告期内，恶意推广类诈骗网站占 51%，位列第一位，其次是赌博类诈骗网站占 22%，情色类诈骗网站占 12%，分别为二、三位。



4. 2017 年中国主要省市访问诈骗网站类型

报告期内，北京、河北、湖南等地区访问的诈骗网站类型以情色论坛为主，广东、黑龙江等地区则以在线赌博为主，辽宁、上海、浙江等地区则以恶意推广为主，其余地区访问恶意软件诈骗网站居多。

2017年中国主要省市访问诈骗网站类型

省份	访问诈骗网站
广东	赌博
辽宁	恶意推广
北京	情色
上海	恶意推广
浙江	恶意推广
福建	恶意推广
江苏	恶意推广
河北	情色
湖南	情色
广西	情色
黑龙江	赌博
四川	恶意软件
山东	恶意推广
河南	情色
河北	恶意推广

省份	访问诈骗网站
重庆	恶意软件
江西	恶意软件
天津	恶意推广
云南	情色
山西	恶意推广
内蒙古	恶意推广
安徽	情色
甘肃	恶意软件
新疆	恶意软件
贵州	恶意推广
海南	恶意软件
宁夏	恶意推广
青海	恶意推广
西藏	情色

5. 诈骗网站趋势分析

2017 年情色、赌博类诈骗网站占比较多，这些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：

Ø 利用微信朋友圈以软文方式进行诱导传播。

Ø 利用 QQ 群发方式进行范围传播。

Ø 利用短信群发平台以中奖方式进行传播。

Ø 利用游戏辅助软件进行传播。

Ø 利用大型互联网平台发布信息进行传播。

6. 2017 年中国挂马网站概述

2017 年瑞星“云安全”系统共拦截挂马网站攻击 540 万余次，北京市受挂马攻击 356 万次，位列第一位，其次是陕西省受挂马攻击 153 万次。

7. 挂马网站趋势分析

2017 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：

Ø 更新到最新的浏览器版本。

Ø 禁止浏览陌生邮件或手机短信发送的链接网址。

Ø 禁止浏览不正规或非法网站。

Ø 禁止在非正规网站下载软件程序。

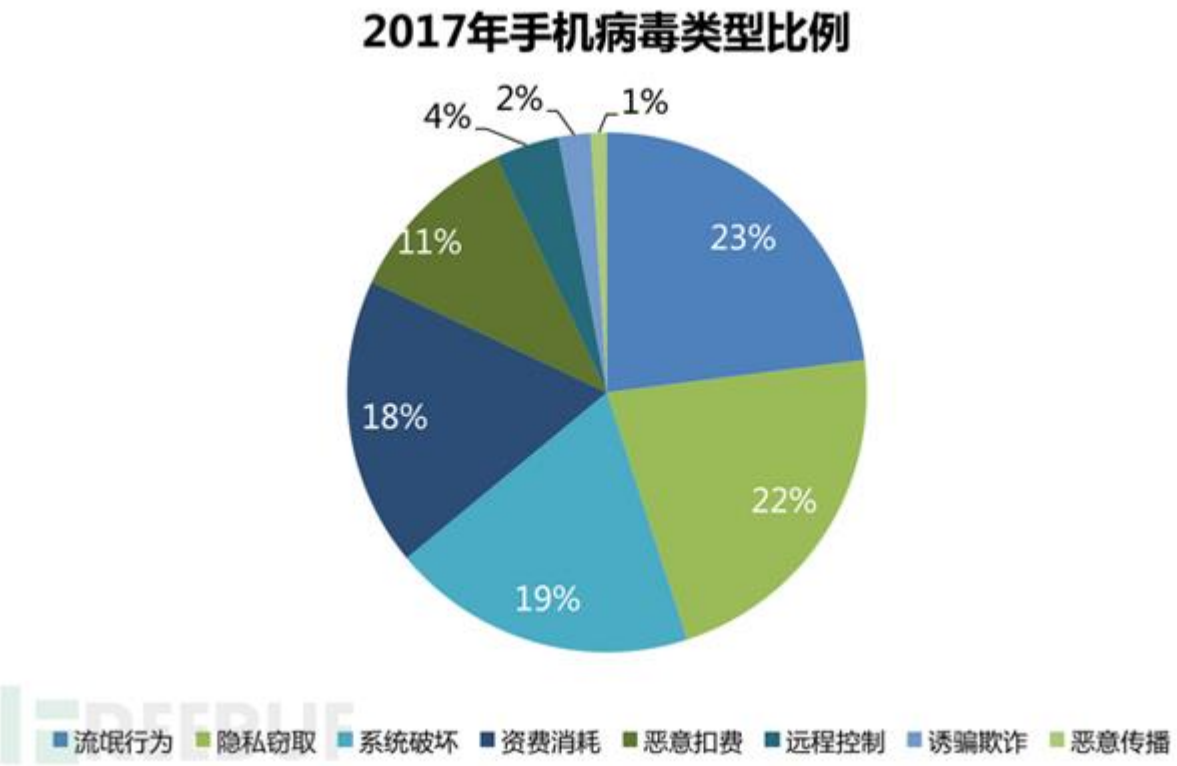
Ø 安装杀毒防护软件。

二、移动互联网安全

（一）手机安全

1.2017 年手机病毒概述

2017 年瑞星“云安全”系统共截获手机病毒样本 505 万个，新增病毒类型以流氓行为、信息窃取、系统破坏、资费消耗四类为主，其中流氓行为类病毒占比 23.3%，位居第一。其次是隐私窃取类病毒占比 22.3%，第三名是系统破坏类病毒，占比 19%。



2.2017 年手机病毒 Top5

2017年手机病毒Top5

序号	病毒名	恶意行为
1	Ransom.LockScreen/Android!8.594	窃取个人帐户信息，通过后门程序取得访问设备功能，锁定或加密设备以致用户必须付费才能解锁设备。
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	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。
4	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，诱导用户触发点击行为。
5	Trojan.Android.Locker!1.A791	伪装成系统更新来申请获得用户管理权限，然后使用随机数字更换用户锁屏PIN码，并向受害者勒索钱财。

3. 2017 年 Android 手机漏洞 Top5

2017年Android手机漏洞Top5

序号	漏洞名称	漏洞编号	简介
1	Janus高危漏洞	CVE-2017-13156	该漏洞允许攻击者任意修改Android应用中的代码，而且不会影响其签名。
2	BlueBorne蓝牙漏洞	CVE-2017-0785	蓝牙协议漏洞，只要手机开启了蓝牙，就可能被远程控制。
3	Android WebView 跨域访问漏洞	CNVD-2017-36682	攻击者利用该漏洞，可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证，在受害者毫无察觉的情况下实现对APP用户账户的完全控制。
4	Android Media framework avc decoder远程代码执行漏洞	CNVD-2017-23420	远程攻击者可利用该漏洞执行任意代码。
5	roadpwn 漏洞	CVE-2017-9417	通过Wi-Fi使安卓手机崩溃。

（二）2017 年移动安全事件

1.共享单车扫码诈骗事件

2017 年 2 月，有人发现共享单车的“扫码骑走”上方还贴着其他二维码，贴上去的二维码扫描之后立刻出现了转账提示！用户手机扫描此类二维码后，或被要求直接转账，或被要求下载可疑软件，致使资金账户面临被盗刷的风险。

2.315 曝光人脸识别技术成手机潜在威胁

2017 年 315 晚会上，技术人员演示了人脸识别技术的安全漏洞利用，不管是通过 3D 建模将照片转化成立体的人脸模型，还是将普通静态自拍照片变为动态模式，都可以骗过手机上的人脸识别系统。此外，315 还揭露了公共充电桩同样是手机的潜在威胁，用户使用公

共充电桩的时候，只要点击“同意”按钮，犯罪分子就可以控制手机，窥探手机上的密码、账号，并通过被控制的手机进行消费。

315曝光人脸识别技术

3.勒索病毒伪装成《王者荣耀辅助工具》袭击移动设备

2017 年 6 月，一款冒充“王者荣耀辅助工具”的勒索病毒，通过 PC 端和手机端的社交平台、游戏群等渠道大肆扩散，威胁几乎所有 Android 平台，设备一旦感染后，病毒将会把手机里面的照片、下载、云盘等目录下的个人文件进行加密，如不支付勒索费用，文件将会被破坏，还会使系统运行异常。

病毒伪装成游戏辅助工具

4.亚马逊、小红书用户信息泄露助长电话诈骗

2017 年 6 月，亚马逊和小红书网站用户遭遇信息泄露危机，大量个人信息外泄导致电话诈骗猛增。据了解，亚马逊多位用户遭遇冒充“亚马逊客服”的退款诈骗电话，其中一位用户被骗金额高达 43 万，小红书 50 多位用户也因此造成 80 多万的损失。

小红书用户信息泄露

5.病毒伪装“Google Play”盗取用户隐私

2017 年 6 月，一款伪装成“Google Play”的病毒潜伏在安卓应用市场中，该病毒会伪装成正常的 Android market app，潜伏在安卓手机 ROM 中或应用市场中诱导用户下载安装。该病毒安装后无启动图标，运行后，会向系统申请大量高危权限(发短信和静默安装等)，随后伪装成 GooglePlay 应用并安装和隐藏在 Android 系统目录下。因为在“/system/app/”路径下的 app 默认都是拥有 system 权限的，所以该病毒样本可以在用户不知情的情况下，在后台静默下载并安装应用到手机当中，还会获取用户手机中的隐私信息，给用户造成系统不稳定或隐私泄露等安全性问题。

6.手机共享充电可能会泄露个人隐私

在公共场合使用免费充电桩充电时，许多人都不太注意手机上“是否开启 USB 调试”或“是否信任该设备”的提示信息，如果用户点击“是”或“信任”按钮，就相当于让充电设备掌握了手机的绝对控制权，黑客就可以随意窃取手机里的信息。

手机共享充电可能会泄露个人隐私

7.安卓爆重大安全漏洞黑客可以任意篡改 App

2017 年 12 月，谷歌通过其官方网站通告了一个高危漏洞 CVE-2017-13156（发现厂商将其命名为 Janus），该漏洞可以让攻击者无视安卓签名机制，通过绕过应用程序签名验证的形式，对未正确签名的官方应用植入任意恶意代码，目前安卓 5.0—8.0 等版本系统均受影响，预计每日上千万的活跃安卓应用将存在被利用可能，巨大的潜在威胁风险使得 Janus 漏洞成为了安卓系统年度大漏洞！

网友安装这些仿冒 App 后，不仅会泄露个人账号、密码、照片、文件等隐私信息，手机更可能被植入木马病毒，进而导致手机被 ROOT，甚至被远程操控。

三、互联网安全

（一）2017 年全球网络安全事件解读

1.The Shadow Brokers 泄露方程式大量 0day 漏洞

2017 年 4 月，The Shadow Brokers 再度放出大量“方程式组织”使用的黑客工具，包括 OddJob、EasyBee、EternalRomance、FuzzBunch、EducatedScholar、EskimoRoll、EclipsedWing、EsteemAudit、EnglishMansDentist、MofConfig、ErraticGopher、EmphasisMine、EmeraldThread、EternalSynergy、EwokFrenzy、ZippyBeer、ExplodingCan、DoublePulsar 等。其中有多个可以远程攻击 Windows 的 0day 漏洞。受影响的 Windows 版本包括 Windows NT，Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8、Windows 2008、Windows 2008 R2、Windows Server 2012 SP0 等。这次泄露的工具也直接导致了后来 WannaCry、Petya 的全球爆发。

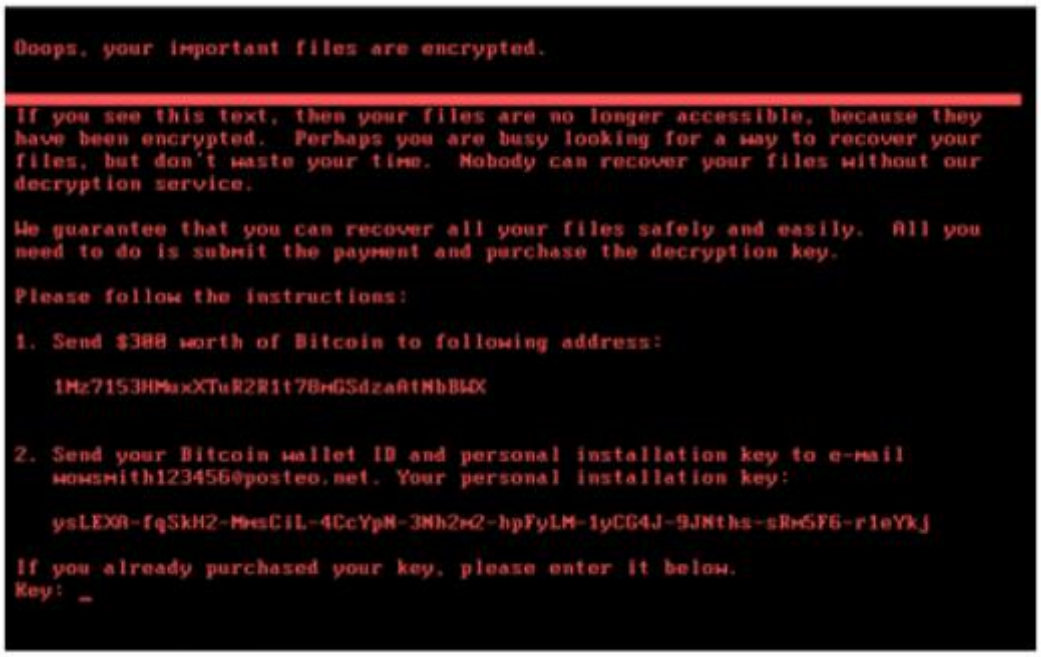
2.WannaCry 勒索袭击全球

2017 年 5 月，一款名为 WannaCry 的勒索病毒席卷全球，包括中国、美国、俄罗斯及欧洲在内的 100 多个国家，我国部分高校内网、大型企业内网和政府机构专网遭受攻击较为严重。勒索软件利用的是微软 SMB 远程代码执行漏洞 CVE-2017-0144，微软已在今年 3 月份发布了该漏洞补丁。2017 年 4 月黑客组织影子经纪人（The Shadow Brokers）公布的方程式组织（Equation Group）使用的

“EternalBlue”中包含了该漏洞利用程序，而该勒索软件的攻击者在借鉴了“EternalBlue”后发起了这次全球性大规模勒索攻击。

3.Petya 病毒借勒索之名袭击多国

2017 年 6 月，一个名为“Petya（中文音译彼佳）”的新勒索病毒再度肆虐全球，包括乌克兰首都国际机场、乌克兰国家储蓄银行、邮局、地铁、船舶公司、俄罗斯的石油和天然气巨头 Rosneft、 丹麦的航运巨头马士基公司、美国制药公司默克公司、美国律师事务所 DLAPiper、乌克兰一些商业银行以及部分私人公司、零售企业和政府系统，甚至是核能工厂都遭到了攻击。影响的国家有英国、乌克兰、俄罗斯、印度、荷兰、西班牙、丹麦等。与 WannaCry 相比，该病毒会加密 NTFS 分区，覆盖 MBR，阻止机器正常启动，影响更加严重。



4.Xshell 和 CClearner 被植入后门

2017 年 7 月，著名服务器终端管理软件 Xshell 在发布的 5.0 Build 1322 官方版本中被植入后门，用户下载或更新到该版本均会中招。由于相关软件在国内程序开发和运维人员中被广泛使用，可能会导致大量用户服务器账号密码泄露。

无独有偶，2017 年 9 月，著名系统优化工具 CCleaner 的某个版本被发现植入后门，大量使用该工具的用户将面临泄密风险。这是继 Xshell 后门事件后，又一起严重的软件供应链来源攻击事件。CCleaner 是一款免费的系统优化和隐私保护工具，主要用来清除 Windows 系统不再使用的垃圾文件，以腾出更多硬盘空间，并且还具有清除上网记录等功能。

5.WPA2 协议曝高危漏洞

2017 年 10 月，国外研究人员 Mathy Vanhoef 在 WPA2 协议中发现严重安全漏洞，几乎影响所有 Wi-Fi 设备，当一台设备加入一个受保护的 Wi-Fi 网络时，一个名为四次握手的流程便会发生，这种“握手”会确保客户端与接入点都能拥有正确的登录信息，并生成一个新的加密密钥来保护网络流量。这个加密密钥会在四向握手的第三步安装，但如果接入点认为消息丢失，有时会重复发送相同的密钥。

研究发现，攻击者可以迫使接入点安装相同的加密密钥，这样便可借此攻击加密协议，并破解数据。攻击者可以利用 KRACK 攻击读取敏感信息，如信用卡账号、密码、聊天信息、电子邮件、照片等。

6.蓝牙协议爆严重安全漏洞

2017 年 8 月，物联网安全研究公司 Armis 在蓝牙协议中发现了 8 个零日漏洞，这些漏洞将影响超过 53 亿设备——从 Android、iOS、Windows 以及 Linux 系统设备到使用短距离无线通信技术的物联网设备，利用这些蓝牙协议漏洞，Armis 构建了一组攻击向量 (attack vector)“BlueBorne”，演示中攻击者完全接管支持蓝牙的设备，传播恶意软件，甚至建立一个“中间人”（MITM）连接。

7.BadRabbit 突袭东欧

2017 年 10 月，新型勒索病毒 BadRabbit 在东欧爆发,乌克兰、俄罗斯等企业及基础设施受灾严重。该病毒会伪装成 flash_player，诱导用户下载，当用户下载后，病毒会加密特定格式文件，修改 MBR，并索要比特币。BadRabbit 可以通过弱口令和漏洞在局域网扩散，成为勒索病毒蠕虫化的典型代表。

8.大量家庭摄像头被入侵

2017 年 6 月，央视曝光大量家庭摄像头遭入侵。很多人家里都装有智能摄像头，下载一个相关联的应用程序，就可以随时用手机查看家里情况，但是由于很多智能摄像头存在弱口令、漏洞等问题，导致大量家庭摄像头遭入侵。一旦攻击者入侵成功，便可以远程观看受害者家中视频。

9.FireBall 火球病毒感染超过 2.5 亿电脑

2017 年 6 月，由中国商业公司控制的 Fireball(火球)病毒，感染全球约 2.5 亿部计算机，感染最严重的国家是印度、巴西和墨西哥。火球病毒通过捆绑正常软件传播，中毒电脑浏览器主页、默认搜索页会被锁定且难以更改，黑客利用广告插件植入广告获利，去年一年获利近 8000 万元。

（二）2017 年 APT 攻击事件

1.白象 APT 组织

白象 APT 组织，又称摩诃草组织（APT-C-09）、丰收行动、HangOver、VICEROY TIGER、The Dropping Elephant、Patchwork。该组织是一个来自于南亚地区的境外 APT 组织，最早由安全公司 Norman 于 2013 年曝光。该组织在针对中国地区的攻击中，主要针对政府机构与科研教育领域。

中国在过去五年持续遭到白象 APT 组织的网络攻击，该组织主要使用鱼叉攻击，同时也使用基于即时通讯工具和社交网络作为恶意代码的投递途径。其攻击使用的恶意代码主要针对 Windows 系统，整

个攻击过程使用了大量系统漏洞，其中至少包括一次 0day 漏洞攻击。

2、越南背景 APT32 攻击亚洲国家

APT32 又称海莲花、OceanLotus、APT32，有信息表明该组织为越南背景，主要针对东南亚国家进行攻击，其中包括越南周边国家的政府、公司等机构，越南被攻击的主要目标为，跨国公司在越南的分公司和全球咨询公司在越南的办事处，以及持不同政见者和记者。

2012 年开始攻击中国的政府、海事机构、科研院所、航运企业等。主要通过水坑攻击和鱼叉邮件进行攻击。水坑攻击下载的样本伪装为浏览器和 flash 更新、字体等。鱼叉邮件攻击中所发送的邮件附件，文件名非常具有针对性，预先对国内时事热点和被攻击单位业务进行了一定的了解，攻击成功率高。

攻击主要特点为：

（1）善于使用白利用，曾利用过谷歌、赛门铁克等公司带有数字签名的软件。

（2）攻击网站较为明目张胆，替换下载链接，植入恶意脚本，伪装 flash 更新，伪装字体。

（3）定制后门和开源工具相结合，善于使用 Meterpreter、Cobalt Strike。

（4）掌握的资源较丰富，提前收集过被攻击者的情报，善于使用社工。

3、Turla 监视全球领事馆和大使馆

Turla 由 BAE 研究员首次发现，又称 Waterbug 、Venomous Bear、Krypton。自 2007 年以来一直处于活跃状态，其主要针对欧洲外交部等政府机构与军工企业展开攻击活动。2017 年 8 月 30 日 ESET 发布研究报告披露，Turla 使用隐秘后门“Gazer”监控全球的领事馆和大使馆。恶意软件 Gazer 由开发人员采用 C++程序编写，经鱼叉式钓鱼攻击进行传播，可由攻击者通过 C&C 服务器远程接收加密指令，并可使用受损合法网站（多数使用 WordPress）作为代理规避安全软件检测。

有趣的是，不仅早期版本的 Gazer 签发了 Comodo 颁发的“Solid Loop Ltd”有效证书，而最新版本也签发了“Ultimate Computer Support Ltd.”颁发的 SSL 证书。ESET 公司在报告中指出，除了将后门与合法 Flash Player 安装程序捆绑在一起之外，Turla 组织使用的 URL 及 IP 地址来自 Adobe 的合法基础设施，从而让受害者误以为自己在下载合法软件。

潜在攻击途径可能包括：

（1）劫持受害者组织机构网络内的设备，利用其充当中间人（简称 MitM）攻击的跳板。

（2）攻击者可能入侵目标网关，借此拦截组织内网与互联网之间的所有输入与输出流量。

（3）流量拦截同样可能发生在互联网服务供应商（简称 ISP）身上，这是 FinFiher 间谍软件在监控活动中使用的一项策略。

（4）攻击者可能已利用边界网关协议（简称 BGP）劫持将流量重新路由至 Turla 控制的服务器，不过 ESET 方面指出该策略可能很快触发 Adobe 或 BGP 监控服务的警报。

4、APT33 窃取能源与航天机密

网络安全厂商 FireEye 公司，2017 年 9 月份披露，某伊朗黑客组织至少自 2013 年来一直针对沙特阿拉伯、韩国以及美国的各航空航天与能源企业开展入侵活动，并将此作为其大规模网络间谍活动的一部分，旨在大量收集情报并窃取商业机密。该组织的主要活动集中在向目标网络发送包含恶意 HTML 链接的钓鱼邮件，旨在利用被称为“TURNEDUP”的一种定制化后门以感染目标计算机。但也有证据表明，该黑客组织亦有能力针对有价值基础设施企业进行数据清除类攻击活动。

APT33 注册有多个域名，并借此将自身伪装为航空公司及欧美承包商。这些网站在设计上尽可能贴近沙特阿拉伯的合法企业，但其中却充斥着大量伪造信息。这些域名亦很可能被应用到网络钓鱼邮件中，旨在强化对受害者的诱导能力。FireEye 公司的调查结果则再次强调，伊朗政府正在持续投入数额可观的资金，旨在建立起一支有能力进行远程情报收集、发动破坏性攻击、窃取知识产权的专业黑客队伍。

5、APT28 利用“网络冲突”进行攻击

Cisco Talos 安全情报团队发现著名的间谍组织 APT28（又名 Group 74、TsarTeam、Sofacy、Fancy Bear…）发起的新一波恶意

网络活动。有趣的是，攻击活动中使用的诱饵文件是关于即将举办的第九届网络冲突会议（Cyber Conflict U.S. conference）的欺骗性传单。2017 年 11 月份举办的 CyCon US 会议是美国陆军军官学校（西点军校）的陆军网络学院、北约合作网络军事学院和北约合作网络防御中心联合组织的。

以往的 CyCon 会议上，来自世界各地政府、军事和工业的 500 多名决策者和专家，以跨学科的方式，从法律、技术和战略角度来交流网络安全相关的议题。鉴于观察到的 APT28 活动所使用的诱饵文件的性质，推断这一活动是针对那些对网络安全感兴趣的人。与以往 APT28 组织的攻击活动不同，此次的诱饵文件不包含 Office 的 0day 漏洞利用，只在 VBA 宏函数中包含一个恶意的 Visual Basic。

6、APT28 利用 0day 漏洞入侵法国大选

APT28 组织被指干扰法国总统大选，对当时还是候选人的马克龙发动攻击。网络安全公司 Trend Micro 通过监控后发现，APT28 至少创建了 4 个不同的域名，且地址与马克龙党派的官方网站十分类似，大概是为了发起网络钓鱼攻击活动。其中一个虚假域名伪装为微软的网址。据在线记录显示，马克龙竞选团队使用 Microsoft Outlook 收发邮件，因此，使用另外一个 Microsoft 云产品的名称创建域名是有意义的。与此同时，一个含有名为“特朗普攻击叙利亚（英文版本）”附件的钓鱼邮件引起了研究人员的注意。研究人员分析后发现这个文档的真实作用是释放 APT28 组织广为人知的侦察工具 Seduploader。为实现这一目的，攻击中该组织使用了两个 0day 漏

洞：一是 Word 远程代码执行漏洞（CVE-2017-0262），另外一个是 Windows 中的本地权限升级漏洞（CVE-2017-0263）。

7、APT28 攻击国际田联

总部位于摩纳哥的国际田联发布公告称，黑客组织“APT28”对国际田联的系统进行了攻击。国际田联 2017 年 1 月联系到一家英国网络安全公司，对国际田联系统进行技术性调查，这家公司随后发现国际田联的系统遭到攻击，黑客组织从文件服务器中取出关于运动员“治疗用药豁免”的元数据，并将这些元数据存储到另一个新建文件中。国际田联表示，尚不确定有经常盗取相关信息的行为，但黑客组织的兴趣和目的显而易见，并拥有随意获取文件内相关内容的途径和手段。此前 APT28 攻击世界反兴奋剂机构的数据库，后者相继披露多批享有“治疗用药豁免”的运动员名单。世界反兴奋剂机构发表声明，称该黑客组织来自俄罗斯的一家网络间谍机构，俄罗斯方面则否认与此攻击之间具有某种联系。

8、FIN7 的网络攻击扩展到一些零售企业

FIN7（也被称为 Anunak 或银行大盗 Carbanak）是目前为止组织最为严密的复杂网络犯罪组织，主要对美国金融机构渗透攻击。自 2017 年初起开始活跃，因攻击美国公司窃取支付卡数据而广为人知。2017 年 3 月，FireEye 发布了一篇名黑客组织 FIN7 的 APT 攻击简报，报告称 FIN7 组织以钓鱼邮件为攻击渠道，在整个攻击过程中，没有使用到 PE 文件，这在一定程度上躲避了安全软件的查杀。落地的文件也进行了技术上的隐藏，而真正的后门程序却以加密的方式存储在

注册表中。组织的攻击利用 DNS 协议的 TXT 字段进行 C&C 通信。2017 年 6 月 FIN7 利用新的无文件多段式攻击瞄准美国连锁餐厅，表明 FIN7 的网络攻击已经扩展到零售企业。

9、伊朗 APT 组织 CopyKittens 大规模间谍活动

2017 年 7 月 25 日，以色列安全公司 ClearSky 研究人员发布一份详细报告，指出伊朗 APT 组织 CopyKittens 针对以色列、沙特阿拉伯、土耳其、美国、约旦与德国等国家与地区的政府、国防与学术机构展开新一轮大规模网络间谍活动。APT 组织 CopyKittens（又名：Rocket Kittens）至少从 2013 年以来就一直处于活跃状态，曾于 2015 年面向中东地区 55 个目标展开攻击。据悉该报告详细介绍 CopyKittens 在新网络间谍活动中采取的主要攻击手段：

（1）水坑攻击：通过植入 JavaScript 至受害网站分发恶意软件，其主要针对新闻媒体与政府机构网站。

（2）Web 入侵：利用精心构造的电子邮件诱导受害者连接恶意网站，从而控制目标系统。

（3）恶意文件：利用漏洞（CVE-2017-0199）传播恶意 Microsoft Office 文档。

（4）服务器漏洞利用：利用漏洞扫描程序与 SQLi 工具 Havij、sqlmap 与 Acunetix 有效规避 Web 服务器检测。

（5）冒充社交媒体用户：通过与目标系统建立信任传播恶意链接。

ClearSky 公司威胁情报负责人伊雅·瑟拉表示，“他们在网络间谍组织当中处于较低水平线，且未使用零日漏洞，他们自主开发的工具在多个层面都要逊于其它同类恶意组织。”

总体而言，该组织的战术、技术与程序（TTP），主要包括恶意邮件附件、钓鱼攻击、Web 应用程序攻击，这些并无亮眼之处，而且直到 2016 年开始才着手利用水坑式攻击。然而，他们获得的持续成功证明，技术水平相对较低但坚持不懈的威胁方仍然能够成功完成目标。

10、Lazarus APT 魔爪伸向加密货币

安全公司 Proofpoint 近日发现 Lazarus APT 组织对加密货币极为关注，并试图利用公众、媒体对加密货币价格暴涨的浓厚兴趣展开攻击。因此 Proofpoint 推断 Lazarus 的攻击行动可能与经济利益挂钩。Lazarus（音译“拉撒路”）堪称全球金融机构首要威胁。该组织自 2009 年以来一直处于活跃状态，据推测早在 2007 年就已涉足摧毁数据及破坏系统的网络间谍活动。由于美国经济制裁的压力，且朝鲜国内军事投入成本需求不断增加，故而，原先以获取政府、军事信息、破坏网络正常运行的大规模的朝鲜黑客组织，如 Lazarus 等，近来已经将视线转向金融机构、赌场、参与金融贸易软件开发的公司、虚拟货币等更为经济型的目标，将窃取到资金转移到朝鲜国内。

四、趋势展望

（一）勒索病毒技术手段愈加复杂

勒索病毒的技术手段在 2017 年有了质的提高，WannaCry、Petya 和 BadRabbit 就是其中的典型代表，不管从传播途径还是加密手段都比以往有很大的提升。勒索病毒在传播上采用蠕虫的方式，通过漏洞和弱口令在局域网内迅速传播。以往的传播手段主要是通过垃圾邮件、EK 工具、网站挂马等，手段被动，效果有限。但通过蠕虫的方式可以化被动为主动，起到“事半功倍”的效果。同时在加密手段上也比以往的有所提升，以往的勒索主要是对文件进行加密，但在 2017 年勒索病毒的手段不单单是对文件进行加密，有的还对磁盘的 MBR 扇区，甚至是 NTFS 文件系统进行加密，造成的破坏性更大。不难想象在未来勒索病毒仍将延续这种趋势，勒索病毒的防范任重而道远。

（二）挖矿类病毒或将迎来爆炸性增长

2017 年注定是数字货币狂欢的一年，比特币的价格从年初的 970 美元涨到年末的 2 万多美元，翻了将近 20 倍，各种其他山寨币也是水涨船高。区块链技术大火，各种 ICO 风起云涌，各种挖矿类病毒也随之爆发增长。

各类网络罪犯通过 2017 年曝出的各种漏洞，如 windows 系统的 MS17-010,Struts2 的 S2-045、S2-046，weblogic 的反序列化漏洞等，疯狂在网络上抓取各种肉鸡。在以往这些肉鸡都会被用来进行 DDOS 活动，但是在今年这些肉鸡大部分都被用来挖矿。数字货币的价值愈大，伴随而来的挖矿攻击活动将愈发频繁。

2017 年随着数字货币的价格上涨，催生出一种使用浏览器挖矿的技术手段 Coinhive，在网页中插入 JS 脚本，当有用户访问该网页，挖矿程序就会在网民的电脑上工作，占用大量系统资源，导致 CPU 利用率突然提升，甚至高达 100%。Coinhive 这种技术的产生，受到黑客们的广泛关注，各路攻击者攻陷正常网站挂载 JS 脚本，替换广告脚本，通过劫持流量和搭建钓鱼网站等手段在用户浏览器疯狂的掘币，严重威胁所有网民的上网安全。

（三）物联网（IoT）设备面临的安全威胁越发突出

IoT 设备最近几年发展神速，但是随之增加的安全问题愈加严峻。这些设备中往往缺乏相关的安全措施，而且这些设备大多运行基于 Linux 的操作系统，攻击者利用 Linux 的已知漏洞，能够轻易实施攻击。致使大半个美国断网的 Mirai，以 DVR 设备为目标的 Amnesia，感染家庭路由器用来“挖矿”的 Darlloz 等病毒都将矛头指向了这些脆弱的 IoT 设备。2017 年 9 月出现的 IoT_reaper 不但可以通过设备的弱口令还能通过设备所曝出来的漏洞进行攻击，这种传播手段将愈加流行，可以预见这些脆弱的 IoT 设备随着爆出来的漏洞越多，安全问题将愈发严峻。

（四）区块链安全迎接新的挑战

区块链是比特币的一个意外发现和产物，被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，区块链是一种基于加密技术的低成本、高安全、可定制和封装的去中心化信任解决工具，也是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术

在互联网时代的创新应用模式。目前，其应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

现在的区块链尽管不断得到研究、应用，依旧存在着一定的安全局限，导致在技术层和业务层都面临诸多挑战。对于区块链中的共识算法，是否能实现并保障真正的安全，需要更严格的证明和时间的考验。采用的非对称加密算法可能会随着数据、密码学和计算技术的发展而变得越来越脆弱，未来可能具有一定的破解性。

在比特币中，若控制节点中绝大多数计算资源，就能重改公有账本，这被称为 51%攻击。真实的区块链网络是自由开放的，所以理论上，区块链上无法阻止拥有足够多计算资源的节点做任何操作。在现实情况下，发起 51%攻击是具有一定可行性的。随着区块链技术和 ICO 在 2017 年的大火，随之而来的安全性在未来将会面临新的挑战。