登录

[ISS 2017]电子数据取证 议题分享一：网络犯罪魔与道：过去、现在、未来

明月为临 / 2017-07-31 09:16:00 / 浏览数 3165 安全技术 资源分享 顶(0) 踩(0)

---

2017年7月26,27日，网络安全生态峰会在北京国家会议中心举行。2017网络安全生态峰会(2017 Internet Security Summit
,简称ISS)始办于2014年，在中央网信办网安局、工信部网安局、公安部网安局指导下，由中国互联网协会、中国网络空间协会、阿里巴巴集团、蚂蚁金服集团联合主办，是

2017
ISS聚焦新型网络犯罪类型、解剖新型犯罪手段，共话中国网络"新安全"。同时，联动社会各行业、各领域，"共担当"新业态下的网络安全责任，并通过社会各行业、各学术

电子数据取证&网络犯罪调查分论坛邀请到全国七位知名专家进行了精彩的演讲。分论坛爆满的场面反应了大家对取证和网络犯罪打击的关注。

精彩议题如下(强迫症顺便吐槽下，对齐的不好看)：

分论坛爆满的场面

---

下面分享其中一个议题：网络犯罪魔与道：过去、现在、未来.

首先解释下分论坛的名字：电子数据取证&网络犯罪调查。在坐的各位很多都是电子数据取证领域的专家，打击网络犯罪的先锋，我一直有这样一个观点，不知是否正确，网

那么我想与大家分享的是网络犯罪过去，现在与将来态势的变化，魔高一尺，道高一丈，魔与道的对决，同时探讨下解决之道。

【网络暗流】

1月12日，中央政法工作会议在京召开，中共中央政治局委员、中央政法委书记孟建柱在会上指出，中国网络犯罪占犯罪总数1/3
，并以每年30%以上速度增长，而在未来，绝大多数犯罪都会涉及网络。网络犯罪将成为世界上每个地方、每个人、每件事的最大威胁。针对当前违法犯罪新趋势新特点，

回顾网络犯罪的发展过程，大家可能并不了解我们国家第一起计算机犯罪是什么时间。考证我国第一起网络犯罪，教科书里是这样写的，1986年深圳破获了我国第一起计算
1986年7月13日，中国发生了第1起被破获的计算机犯罪案件。作案者是中国银行深圳分行蛇口支行会计兼电脑控制机主管员陈新义和中国银行深圳分行东门支行会计苏庆忠
不是严格意义上的网络犯罪，所以这个定于用的是用计算机犯罪来。

时间来到了2006年，很多人都对这个可爱的小熊猫图标记忆尤新吧。熊猫烧香病毒被评为2006年毒王，感染百万台机器，造成大量数据被破坏，编写者李俊也成为大家口中
"金元宝棋牌"网络游戏平台非法获利数百万元，涉及赌资达数千万元。丽水公安局将李俊等17人抓获，当然这是后话了。实际上在熊猫烧香案中，已经形成了庞大的犯罪链

这一时期网络犯罪套路日渐成熟，他们追逐的两大目标，一个是数据，一个就是流量。但相应的法律法规远远没有跟上犯罪的发展，据说很多安全圈大佬的安全之路就是从2

□ 十年之后的2016年，徐玉玉案获得了大家的广泛关注。这个案例从专业化的角度来看并不是那么复杂，他们从网上买来数据，数据是黑客从某报名信息平台当中窃取的

实际上2016年暑假还有两起学生被诈骗不幸去世这样的新闻。细究之下，他们分别采用了不同的犯罪手法。

同样是山东临沂发生的宋振宇被诈骗案，宋振宁手机上接收到一条显示发自"95599"的短信，称他的一张信用卡将被扣除1980元的年费。于是就拨打短信中留下的电话，假冒

广东省惠来县高考录取新生蔡淑妍接到不法分子假冒"奔跑吧，兄弟"栏目组发出的虚假中奖短信，蔡淑妍回拨短信中的电话号码，被嫌疑人诱骗点击登录钓鱼网站，并填入相

这三个令人心痛的案例告诉我们，网络诈骗的专业化运作早已成熟，而且带有鲜明的地域特色。

这是网络诈骗如此风行的形势下一些重点的地区，台湾也是非常重要的一个诈骗输出地。

2017年发生了一个特别典型的案例，受害人不知不觉的时候他的钱已经没有了，也没有什么明显的征兆。盗窃分子从网上购买受害人个人信息四大件（身份证、银行卡、密

这个案例是我们应该关注的一个方向。相当长时间以来，我们对个人信息的保护意识不足，打击治理也不是非常到位，造成我们个人的信息已经是相当的泛滥。我想我们没有

在网络暗流当中可以看到各种形形色色的团伙，他们的目标就是一个，钱。钱是建立在流量和数据的基础上。

我们可以把整个网络的暗流分为三个层次，首先第一个层次就是基础的设施，既然要实施网络的诈骗，必然要有一个域名，网络的接入，存储的空间、支付的流通、通讯的

当然，网络诈骗作为一类网络犯罪，是目前我们最关注，打击力度最大的，但并不是网络犯罪的全部。从网络作为犯罪的对象，到网络作为工具，再到网络作为犯罪空间，

【魔之进化】

网络犯罪的进化速度是超出我们想象的，例如广西宾阳，诈骗主业是通过恶意代码等等进行盗号，最新犯罪手法是通过安装木马，拦截短信，进一步实施犯罪的。整个犯罪

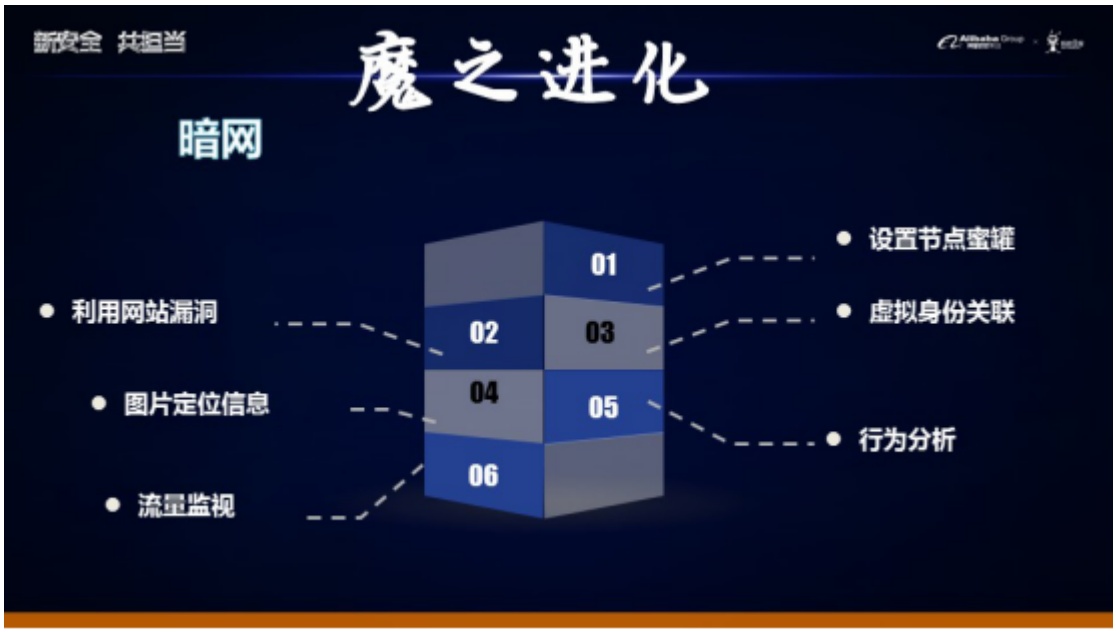
而且现在还有一个趋势就是网络犯罪即服务，原来我们可能需要有一些技术的基础才能够实施一些诈骗行为，比如真正搭个网站得找人帮忙搭，现在我们只需要享受恶意软

而且前两天看到一个新闻，AI技术已经用在了网络犯罪的领域，打码平台，原来是人工打码，很多人一分钟可以打好多，这是人海战术，而现在更先进的一种打码方式，通

而我们业内安全的一些基础已经被突破，比如身份认证，很多应用要求要上传手持身份证的照片，这样一种验证机制甚至我们手机号验证码验证机制都不是特别完美，我们

另外借助暗网的犯罪将会是未来打击的难点，FBI
对Alphabay的追踪我们都看过了，而我们国内对这方面刚刚开始，没有相应的研究。Alphabay的覆灭很大一个原因是网站管理员使用了非匿名的邮箱，同时还有卧底侦查。

我曾在CCFC上介绍过暗网的情报分析思路，大概的方法有一下几种：




总之，网络犯罪的进化速度之快，很多时候是让人瞠目结舌，应接不暇的。只靠被动的打击，只能是疲于应付。那么，我们该如何去应对？

【道法自然】

我们真的能完全相信自己的眼睛吗？我们看到很多表象的东西都是经过犯罪分子层层伪装的，我们可以看一下这几个短信，你能一下子分辨出来它到底是真还是假吗？有几位

所谓道法自然，也就是充分了解犯罪规律，建立数据模型，进行溯源、预警。例如，犯罪分子通过改号软件进行诈骗，那么我们能否建立改号、拨打时间、拨打规律、设备使

【合纵连横】

国务院批准建立由公安部、工信部、中宣部、中国人民银行等23个部门和单位组成的打击治理电信网络新型违法犯罪工作部际联席会议制度。各成员单位各司其职，做好管控

大量的数据掌握在互联网企业手中，大家需要打破藩篱，做到网络犯罪威胁情报的共享与融合，网络空间安全需要大家共同的努力。国际刑警组织积极探索网络情报公私营合

通过警队内部的协作机制，互联网企业积极主动的进行警企协作，建立和完善网络犯罪威胁情报共享，实现社会共治，才让网络环境更加安全。

新安全，新担当，让我们共同努力！


上一篇：[ISS 2017]电子数据取证 ... 下一篇：CSA云安全指南V4.0中文版

1. 0 条回复
   - 动动手指，沙发就是你的了！