第5部分——系统安全

Part V: Management Information Systems Safety and Security

刘跃文 博士 Dr. LIU, Yuewen

教授、博士生导师 Professor

liuyuewen@xjtu.edu.cn

西安交通大学管理学院

School of Management, Xi'an Jiaotong University

V2.0, 2023-Oct


Surface Web
明网
YAHOO!
Google
reddit
CNN.com
bing
Deep Web
深网
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific repositories
Dark Web
暗网
TOR
Political protest
Drug trafficking
and other illegal activities
96%
of content on the Web (estimated)

系统安全性

- 系统安全 System Safety：是指在系统生命周期内应用系统安全工程和系统安全管理方法，辨识系统中的隐患，并采取有效的控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。
- 系统能实现的功能越多，停摆时带来的损失就越大。

例如：5G的便利与安全挑战

当5G打破的网络边界，进一步实现网络世界和物理世界融合时，针对虚拟世界的攻击都将变成物理性伤害，网络攻击的影响力指数级暴涨。

eMBB	大宽带：10GB/s的下载速率，令3D、超高清视频等大流量移动宽带业务成为可能；	大宽带同时也为黑客快速获取数据提供了充分的便利。
uRLLC	高可靠低时延：5G理论延时是1ms，让无人驾驶、工业自动化等业务不再止步于电影；	与车联网、远程医疗、工业自动化、智能电网等重要垂直行业结合时，网络攻击对象及权益进一步扩大；
mMTC	海量大联接：5G单通信小区可连接的物联网终端数量理论值已达百万级别。	更多关键基础设施和重要应用架构在其5G上时，这些高价值目标或将吸引更大的攻击力量——国家级黑客入场。

提纲 Outline

- 系统越强大 组织越脆弱
- 勒索与系统攻击
- 钻系统的漏洞
- 将系统用于服务犯罪

1. 系统越强大 组织越脆弱

1. 案例：武汉协和金银湖院区系统崩了

- “医院的信息系统早上8：30左右就坏了，现在无法读取电子就诊卡，医生电脑收不到任何患者信息，也无法开检查单或处方，不能做治疗……候诊的患者和家属只能在大厅里等着，医生们也不知如何应对。”8月27日，家住湖北省武汉市东西湖区的陈路（化名）向记者反映了他在武汉协和医院金银湖院区的就诊经历。

系统坏了，无计可施

- “这家医院的挂号系统很方便，手机上挂号、绑定就诊卡之后，凭借手机上收到的挂号信息直接去科室分诊台报到、候诊就可以。”陈路表示，系统给出的建议就诊时间是上午9:50，他便提前十分钟赶到了科室楼层。
- 然而，分诊台的护士告诉他，医院的信息系统8:30左右就坏了，无法读取电子就诊卡，也不能开处方和做治疗。候诊的患者和家属只能在大厅里等着，医生们也不知如何应对。“有个就诊的患者告诉我，他已经等了一个多小时了。”陈路说。
- “这一片区域有口腔科和皮肤科的候诊患者，由于医生没法看诊，很多患者和家属都滞留在这里了，为了疫情防控，医院要求隔座就坐，等候区几十人，座位基本都快坐满了。”陈路回忆，期间也有医生从诊室里走出来问分诊台的护士怎么办，但彼此都无计可施。

手动登记

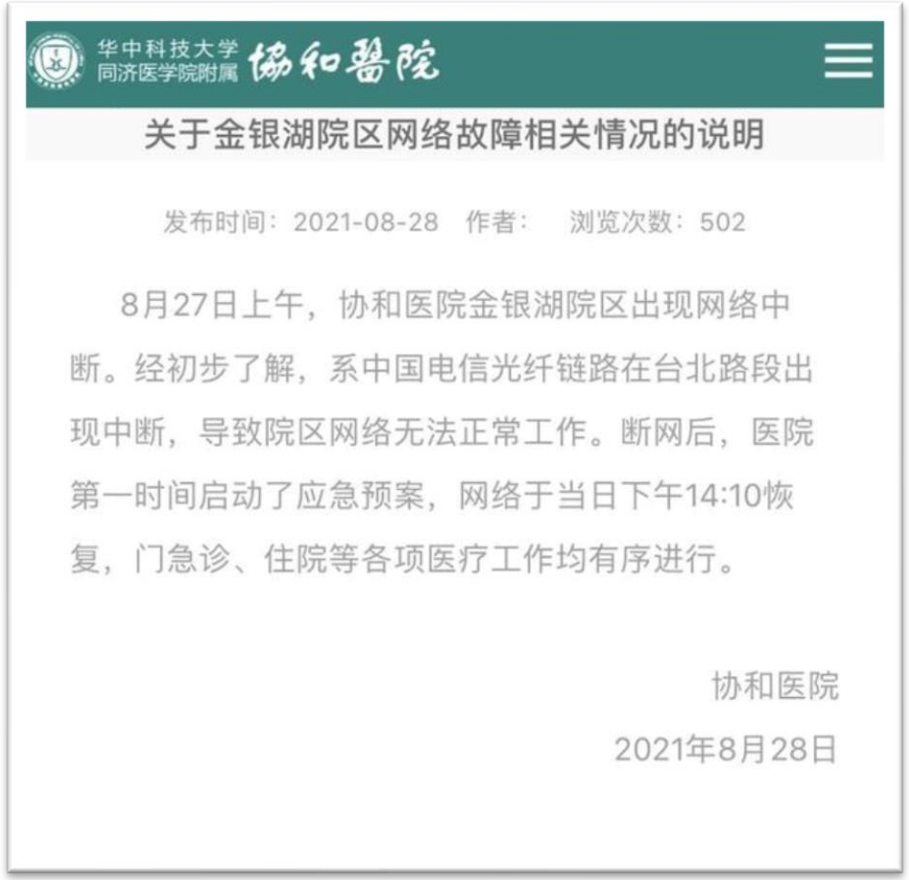
- 10:30左右，系统依然没有恢复，但是医生暂时恢复了诊疗。分诊台的护士招呼候诊的患者手动登记信息，陈路拿到了他的“叫号条”，上面用黑色笔写着他的就诊序号。
- “大约等了不到一个小时就轮到我就诊了，由于系统没好，医生只能手写病历，但是没法开单做检查。”陈路告诉记者，他的病情需要做b超后确认手术方式，但医生没法在系统里开检查单，便告诉陈路自己下午在另一院区也有门诊，让他到那边重新挂号做检查。
- 这就相当于白跑了一趟，还多等了两个小时。“系统崩了连退号都不行，手机退号只能在就诊前一天16:30前，就诊当天退号必须在医院窗口退，因此我也无法退号。”陈路无奈地说，后来，护士开始手动登记退号信息，等系统恢复后再给他们办理退号。

应急准备

- “系统崩溃，就连门诊都没法看吗？难道过去没有电脑和互联网的年代，诊疗就无法进行吗？”陈路无奈地说，医院的各流程都电子化了，线上挂号，读卡候诊，电子病历，电子处方……一旦电子系统出问题，医院就进入了停摆状态。面对停电、停网等突发情况，医院应该有一些准备，保证医疗秩序的稳定。

系统停摆的原因

- 8月27日上午，协和医院金银湖院区出现网络中断。经初步了解，系中国电信光纤链路在台北路段出现中断，导致院区网络无法正常工作。断网后，医院第一时间启动了应急预案，网络于当日下午14:10恢复，门急诊、住院等各项医疗工作均有序进行。
- 该院相关负责人表示，医院在第一时间启动了应急预案和手工流程，并为急诊患者开通了绿色通道，手工流程实施过程中给部分门诊就诊患者带来了不便，但急诊和住院患者的救治及手术皆正常进行，并未受到影响。


华中科技大学同济医学院附属协和医院

关于金银湖院区网络故障相关情况的说明

发布时间：2021-08-28 作者： 浏览次数：502

8月27日上午，协和医院金银湖院区出现网络中断。经初步了解，系中国电信光纤链路在台北路段出现中断，导致院区网络无法正常工作。断网后，医院第一时间启动了应急预案，网络于当日下午14:10恢复，门急诊、住院等各项医疗工作均有序进行。

协和医院

2021年8月28日

其它一些案例

- 在2006年，在美国，大约有350,000个心脏起搏器和123,000 IDC（植入式心脏除颤器）被植入患者体内。2006年是个特别重要的年份，因为在这年，FDA 批准了全基于无线连接控制的医疗设备的临床应用。如今已有300万具心脏起搏器和170万个心脏除颤器处于使用状态。

- 2012年10月，澳大利亚墨尔本的计算机安全会议上，杰克播放了一段录像，演示他如何用一台笔记本电脑在15.2米外遥控心脏起搏器，让它瞬间产生830伏特电压，这足以致人于死地。他还说，也许能设计出针对某一品牌心脏起搏器和除颤器的“蠕虫”病毒，在一定距离内会从一个设备传染另一设备，从而控制一个又一个患者。

- 2013年，身为“明星黑客”的杰克重出江湖，打算在7月31日开幕的“黑帽”黑客会议上，展示一项更为惊人的“黑客绝技”——在9米之外入侵植入式心脏起搏器等无线医疗装置，然后向其发出一系列830V高压电击，从而令“遥控杀人”成为现实！杰克声称，他已经发现了多家厂商生产的心脏起搏器的安全漏洞。

- 《植入式医疗设备：黑客入侵人类》

“这次演讲，将关注于无线植入医疗设备的安全性。我将讨论这些设备的操作和通讯原理，以及通讯协议上的安全漏洞。我们的研究，将揭示如何通过一个普通的数据收发机,来搜索和入侵附近的医疗装置。我也将讨论如何改进这些设计，以增强它们的安全性”。

IOActive, Inc
@IOActive

Follow

Lost but never forgotten our beloved pirate, Barnaby Jack has passed. He was a master hacker and dear friend. Here's to you Barnes!

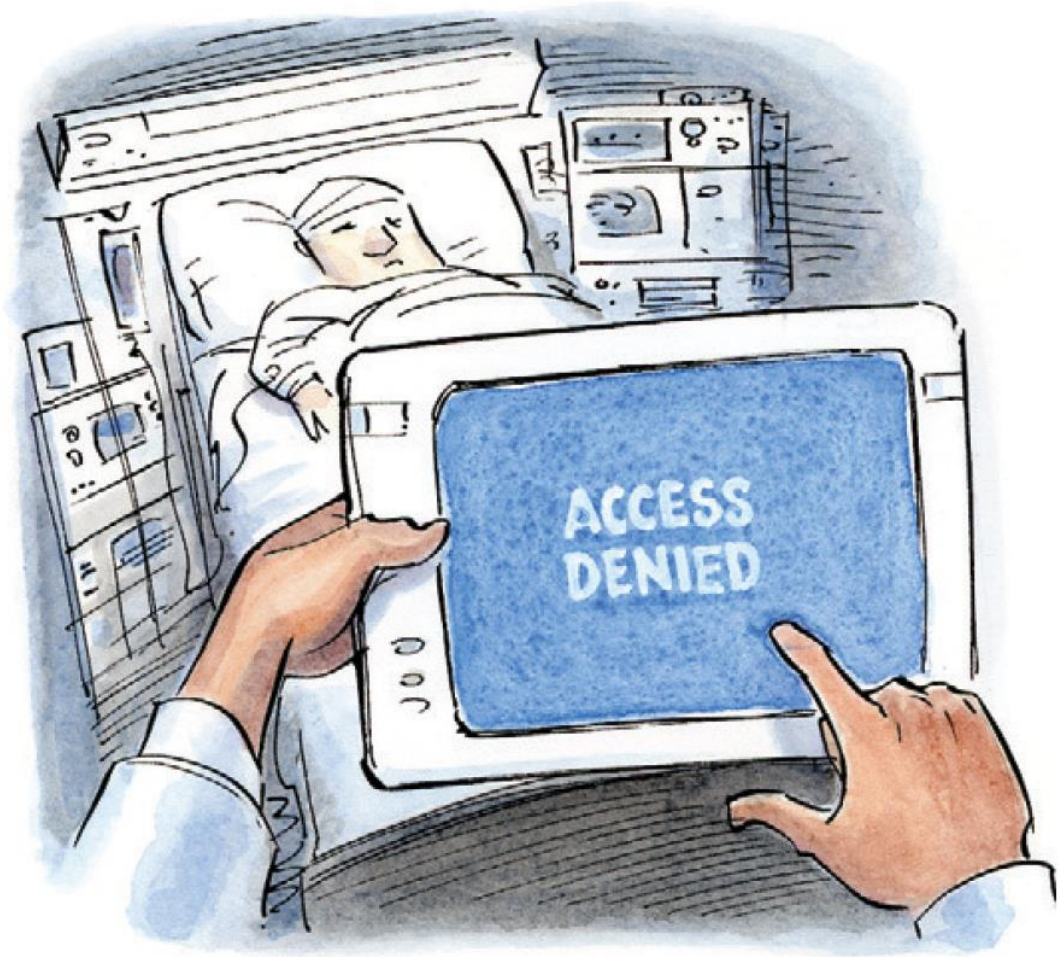
6:58 PM - 26 Jul 2013

267 RETWEETS 52 FAVORITES

- 福特翼虎、丰田普锐斯被黑客找到漏洞、控制行车系统突然加速、刹车、转动方向盘的同期，大众旗下多款车型也被密码学家发现漏洞，可以被黑客轻松开锁点火，扬长而去，就像车钥匙被人拿走一样。此外，市面上多数导航仪能被远程Hacking，这意味着拥有电子锁、点火系统、GPS等智能设备的汽车安全问题将日趋严重。

2. 勒索与系统攻击

1. 案例： Sunnylake医院



背景信息

- Paul是Sunnylake医院的CEO，已经履任5年。
- Paul上任之初的首要目标之一，是将医院的记录系统，从纸质文件转换到电子记录。
- Paul雇佣了Jacob Dale，作为医院IT部门的负责人。IT部门成功地实施了电子化这一目标，建设了Electronic Medical Records（EMRs）系统
  - 初期部分医生抵制这一系统
  - 后期最顽冥不化的老医生都承认：这一系统可以自动检查医疗事务与药品反应
- 这一举动使得Sunnylake医院从一个停滞不前的乡下小医院，一跃成为全国闻名的小医院典范。
- Paul开始时担心病人的数据隐私问题。3年过去了，没有发生任何事情。因此，Paul开始对系统有信心，觉得安全不是大问题。

第一封邮件

- 星期五下午，CEO Paul收到一封匿名邮件：

Ur network security sucks.
But we can help u.
for 100K cash well insure your little hospital dont suffer any disasters.

你的网络安全太烂了！
但是我们能帮助你！
只需要10万美元，
就能让你的医院不遭受任何的灾难！

第二封邮件

- 星期一上午8:00，

We warned u.

我们警告过你哦

Access Denied （访问被拒）

- 医院像往常一样忙碌！

- 医疗记录系统无法访问！
- 黑客搞定了整个EMR系统，把这个系统拉下线！
- 尝试访问这一系统的人，都会看到同样的内容：“*Access Denied*”
- 医生们都挤到IT部门的门口……

第三封邮件

- Jacob去找Paul，此时第三封邮件寄到：

We bet u want your stuff back.
probly shud have protected it better.
for the small price of 100K well
make this go away.

我们觉得你肯定希望你的员工回到工作岗位上
也许你现在后悔，系统应该保护得更好！
只需要10万美元这么一丢丢钱
我们就能让所有的事情正常。

怎么回事儿？

- 黑客使用了一种基于系统的勒索软件，索要一笔赎金10万美元，来交换解密工具。
- 勒索软件禁止访问电子病历记录，甚至系统管理员也无法访问。
- 过去三年中，安全技术发展迅速，但是医院并没有相应更新。可能是某个员工认为在下载“杀毒软件”或者更新软件时，黑客趁机入侵。
- 数据在网络上都有备份，因此不会丢失。但是，此时此刻，医院无法获取数据，被迫进入“静止”状态！

IT部门

- IT部门觉得他们肯定能夺回系统的控制权。
  - 不能支付黑客这笔钱，因为黑客不可信！
  - 我们对系统更了解，黑客只是赢在出其不意上！
  - 但是，需要一些时间才能打赢这场战斗！

  - IT部门尽全力修好了系统2次！
  - 黑客立即反击，重新把系统黑了！

法律顾问

- 医院首席法律顾问Lisa Mankins，希望立即解决这个问题，就算付赎金也可以！

  - 年轻的医生们手足无措，年老的医生们也忘了怎么开药！
  - 依据过时的记录来处理最紧急的病例，会有风险！

  - 已经有一个病人被给错了药，幸运的是，反应是轻微的。
  - 如果医院在缺失记录的情况下发生任何错误，损失的都可能会是病人的生命！
  - 我们没有时间！多拖一个小时，风险就大一分！

  - 医院有保险能支付赎金带来的损失。
  - 损失的不过是一小笔预算而已！

办公室主任（Chief of Staff）

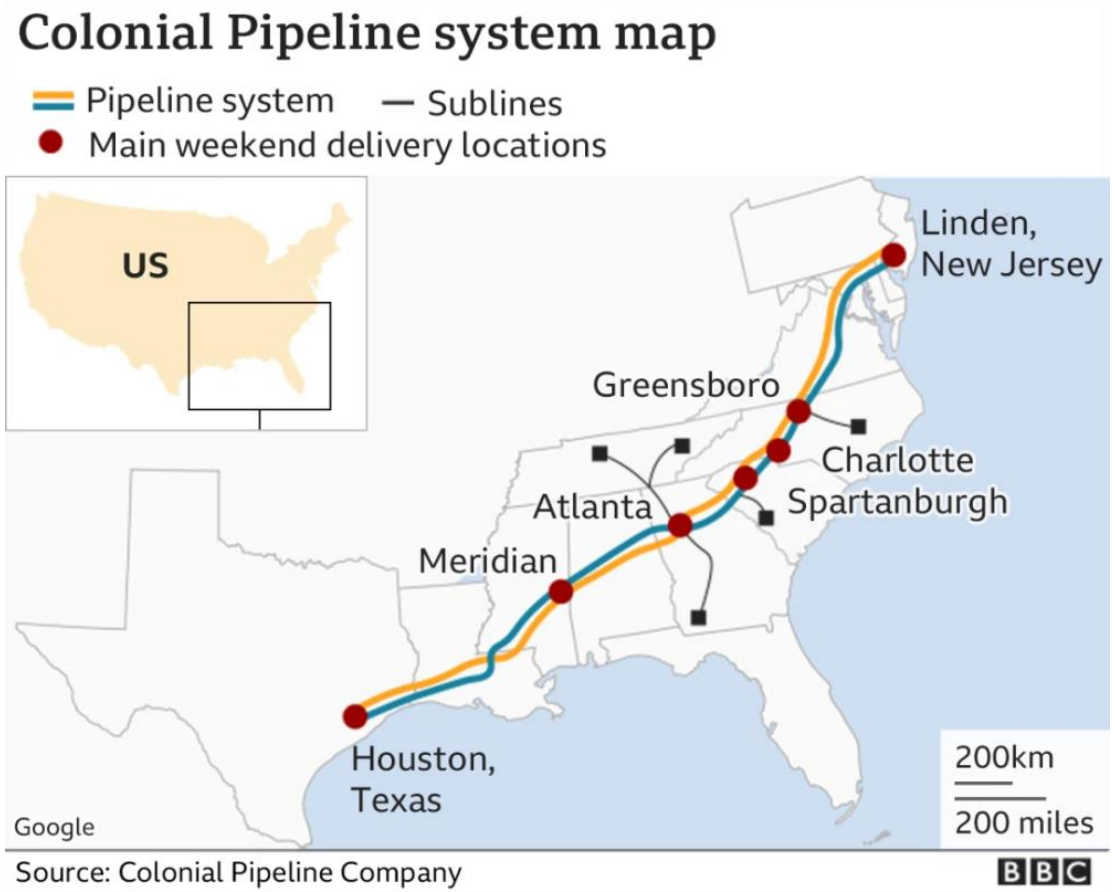
- 你知不知道这事儿后果有多严重？
- 你要是不能立即搞定这件事，我们就回到用纸记录信息的方式！

Paul, I'm never touching one of those damn devices again. And I know plenty of others here who will feel the same way.


如果你是Paul
你该怎么办？

2. 案例：美国最大燃油管道遭受勒索攻击

- Colonial Pipeline是美国最大的成品油管道，每天通过管道系统输送超过1亿加仑的燃料。
- 该管道系统连接得克萨斯州休斯顿和新泽西州林登，跨度长达5500多英里。
- 美国东海岸45%的燃料都由该管道系统提供，此外Colonial Pipeline还为美国军方提供精炼石油产品，例如汽油、柴油、喷气燃料。



- 2021年5月7日（周五） Colonial Pipeline公司声明：
- 5月7日，Colonial Pipeline公司发现遭受网络攻击。此后，我们确定该事件涉及勒索软件。作为响应，我们主动使某些系统脱机以控制威胁，该攻击暂时停止了所有管道的运行，并影响了我们的某些IT系统。得知此问题后，一家领先的第三方网络安全公司被聘用，他们已经对该事件的性质和范围进行了调查，该调查正在进行中。我们已经联系了执法部门和其他联邦机构。
- Colonial Pipeline正在采取措施来解决此问题。目前，我们的主要重点是安全高效地恢复服务以及努力恢复正常运行。此过程已经在进行中，我们正在努力解决此问题，并最大程度地减少对我们的客户以及那些依赖Colonial Pipeline的客户的干扰。

- 5月9日（周日），美国宣布进入国家紧急状态，原因是东欧一个犯罪团伙在5月7日对美国最重要的燃油管道运营商Colonial Pipeline发起了勒索病毒攻击，导致Colonial Pipeline关闭其美国东部沿海各州供油的关键燃油网络。
- 美国交通部发布针对17个州和哥伦比亚特区的紧急声明，宣布放宽道路运输燃油的限制。
- 相信这是美国史上能源基础设施遭受的最大规模网络攻击，如事态持续恐令汽油价格飙升。

- 5月10日（周一）FBI指认Darkside是幕后黑手。
- DarkSide回应只为敛财，没有政治意图，也无意破坏社会；
- Colonial预计到本周末将大幅恢复服务；亚特兰大、北卡罗莱纳州等地有消息称汽油供应已出现短缺，加油站排起长队；
- 5月11日（周二），Colonial Pipeline官网关停。

- 据安全公司Cybereason在2021年4月出具的一份报告显示，DarkSide自2020年8月开始活动，以RaaS（勒索软件即服务）的模式运营，擅于横向移动并攻击拿到域控制器（DC）致使整个网络环境陷入瘫痪。
- 目前该组织已发布40多家受害单位的“未赎回”数据（实际受害者数量应该更多），并要求他们提供20万至200万美元的赎金。

- 世界经济论坛网络安全中心的网络战略负责人阿尔吉德·皮皮凯特针对本次事件发表了自己的见解：“安全脆弱性已成为系统性问题，除非将网络安全嵌入开发阶段，从源头解决安全问题，否则针对石油和天然气管道或水处理厂等工业系统的攻击事件只会越来越多。”

- 该公司不得不向黑客支付了440万美元的赎金，以恢复被攻击的系统。
- Colonial Pipeline公司首席执行官布朗特在上个月接受《华尔街日报》的采访时表示，该公司之所以遵守了440万美元的赎金要求，是因为不知道黑客入侵的程度以及恢复所需时间。但私底下，该公司已经采取了早期措施并通知了FBI，并按照指示帮助调查人员追踪到了黑客使用的加密货币钱包。

- 2021年6月7日，美国司法部副部长丽莎·莫纳表示，美国调查人员已经追回了63.7个比特币，价值230万美元——这是已支付赎金中的“大部分”。这也是美国司法部最近成立的数字勒索特别工作组首次追回的赎金。
- 在美国与黑客攻击勒索的持续斗争中，这是一场重大胜利。但美国司法部对他们究竟是如何做到的却是含糊其辞。他们只是说，黑客比特币钱包的“密钥”在“联邦调查局手中”。有了这把密钥——实际上是一个密码，特工们可以很简单地登录并将数字货币发送到他们控制的另一个钱包。

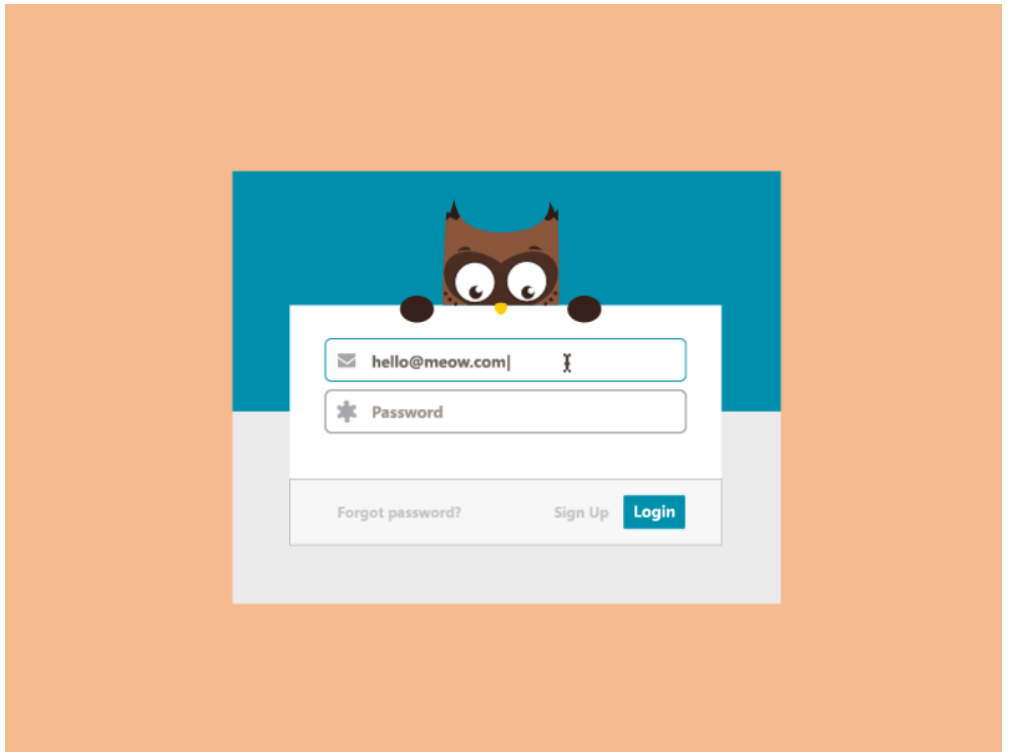
同类事件

- 2021.2 美国佛罗里达州的一家水处理厂遭黑客攻击，攻击者通过一个允许授权用户远程访问的程序，远程进入了监测水处理相关化学物质含量的电脑系统。
- 2020.10 美国俄勒冈州一家医院 Sky Lakes Medical Center在勒索软件攻击后关闭了计算机系统，严重影响医院正常运营，造成经济损失。
- 2020.5 中国台湾两个最大的炼油厂（CPC和FPCC）两天内相继遭遇网络攻击，波及整个供应链，甚至影响到在加油站加油的客户。
- 2020.2 美国某天然气运营商遭到勒索攻击，导致该工厂IT与OT网络数据被锁定，被迫停摆2天，并被国土安全部通报。
- ……

3. 各种系统攻击的手段

（1）SQL注入式攻击

- 例如：原本验证用户名的SQL语句为
  - select * from userinfo where id=‘用户名’;
- 你填入用户名：
  - 用户名’; delete from userinfo where ‘1’=‘1
- 如果系统没有防范，就变成了：
  - select * from userinfo where id=‘用户名’; delete from userinfo where ‘1’=‘1’;
- 数据库里的数据就被删光了！



假设这个路由登录页面，是通过拼接字符串的方式构造动态sql语句，然后到数据库中校验用户名密码是否存在，假设其后台sql语句是：

```
sql='select * from users where user='&user&' and passwd='&passwd&'
```

那么我们使用admin做用户名，用'1' or 'a'='a来做密码的话，那么查询就变成了

```
select * from users where user= ‘admin’ and passwd='1‘ or 'a'='a'
```

这样的话，根据运算规则（先算and 再算or），最终结果为真，这样就可以进到后台了。

SQL注入攻击危害

- 收集数据库的类型、结构等信息为其他类型的攻击做准备。
- 数据库信息泄漏：数据库中存放的用户的隐私信息的泄露。
- 数据库被恶意操作：数据库服务器被攻击，数据库的系统管理员帐户被窜改。
- 网页篡改：通过操作数据库对特定网页进行篡改。
- 网站被挂马，传播恶意软件：修改数据库一些字段的值，嵌入网马链接，进行挂马攻击。
- 服务器被远程控制，被安装后门。经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统。
- 破坏硬盘数据，瘫痪全系统。

这是一张相当有技术含量的号牌遮挡，其对交警系统SQL Injection的hack案例。当摄像头拍到你车牌号并把其转成文本后，插入数据库时的SQL注入。看到了吧，千万别惹程序员。

（2）系统安全威胁——木马

- 基本含义：隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序。
- 种类：网游木马；网银木马；下载类；代理类；FTP木马；通讯软件类；网页点击类。
- 特征：隐蔽性、欺骗性、顽固性、危害性。
- 传播方式：下载；系统漏洞；邮件；远程连接；网页；蠕虫病毒。

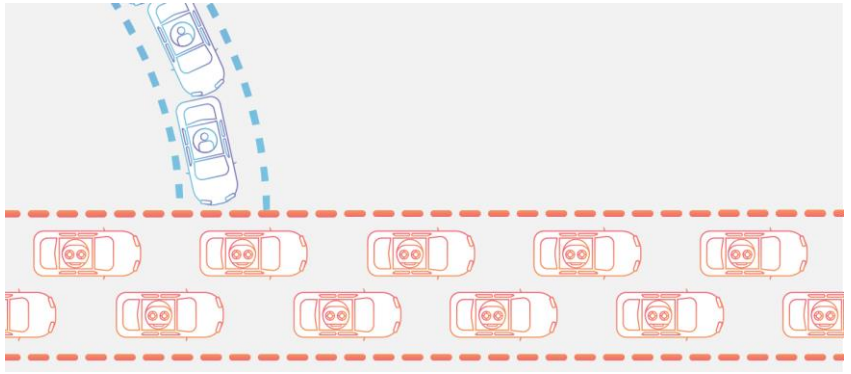
视频：手机木马能干什么

视频：利用共享充电宝下木马

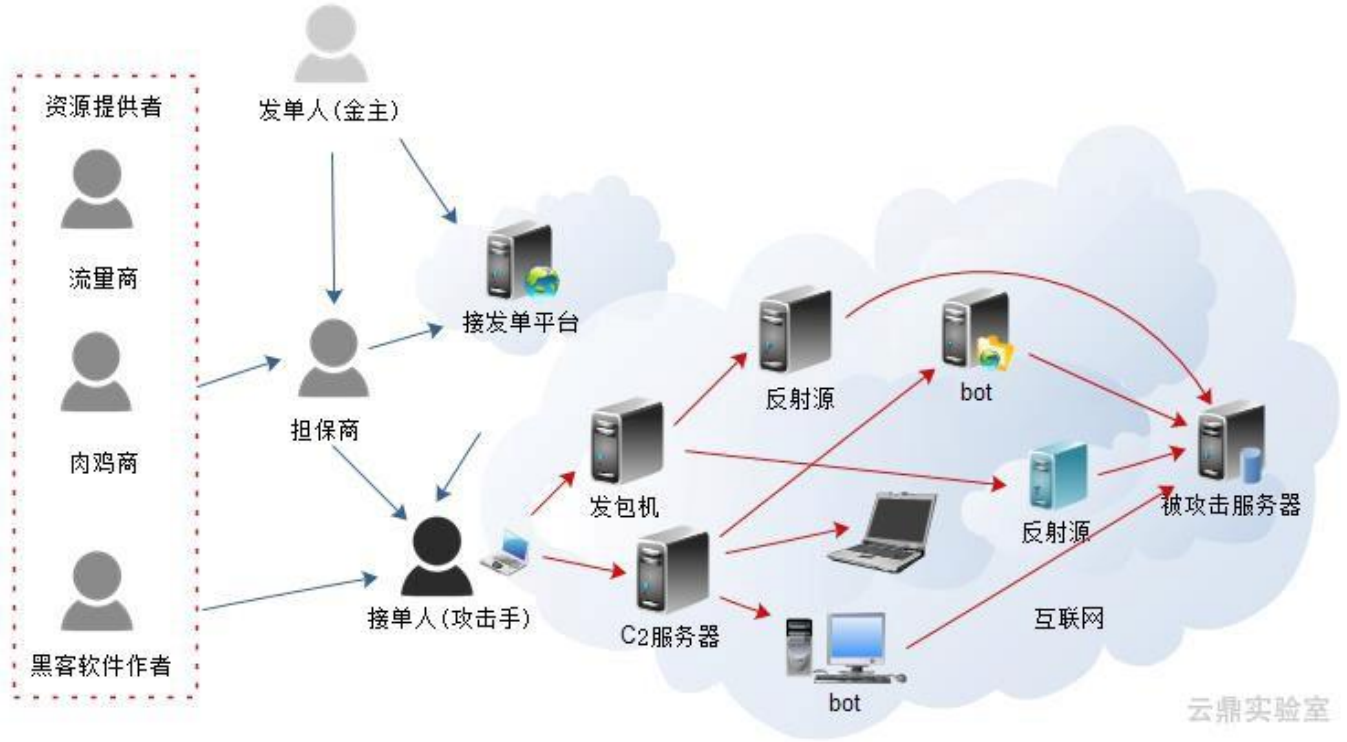
共享充电宝是真的有“毒”

（3）DDoS攻击

- 分布式拒绝服务攻击(Distributed Denial of Service)，指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。
- 攻击者利用“肉鸡”（傀儡机，受黑客远程控制的机器）对目标网站在较短的时间内发起大量请求，大规模消耗目标网站的主机资源，让它无法正常服务。



- “肉鸡”，可谓是DDoS攻击的核心大杀器。这里提到一点，实践证明，目前并不是只有PC会成为“肉鸡”，现在可以这样说，只要是物联的设备都有可能成为肉鸡，比如：手机、服务器、智能音响等等。

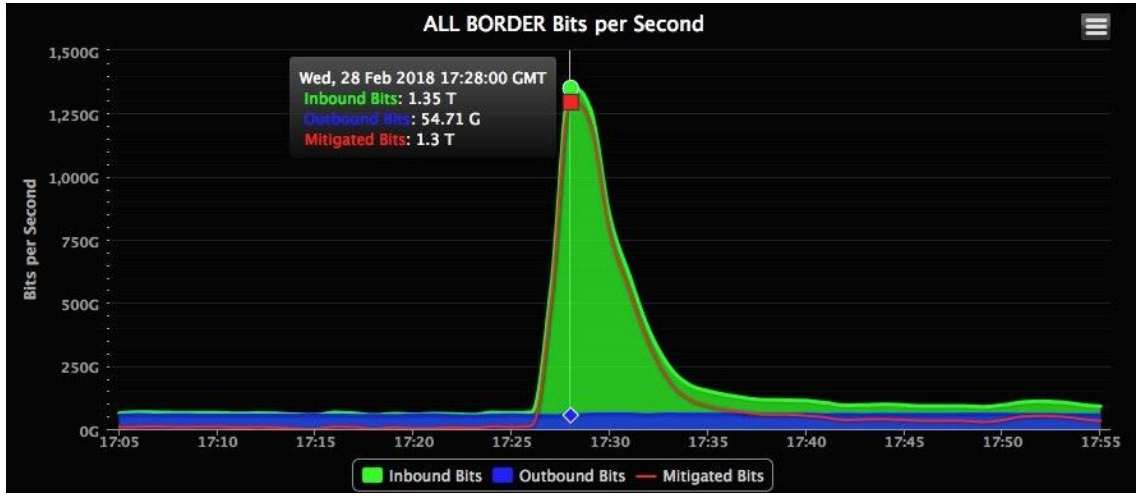


DDoS攻击种类

- 畸形报文：包括Frag Flood、Smurf、Stream Flood、Land Flood、IP畸形报文、TCP畸形报文、UDP畸形报文等。
- 传输层DDoS攻击：包括Syn Flood、Ack Flood、UDP Flood、ICMP Flood、RstFlood等。
- DNS DDoS攻击：包括DNS Request Flood、DNS Response Flood、虚假源+真实源DNS　Query Flood、权威服务器攻击和Local服务器攻击等。
- 连接型DDoS攻击：包括TCP慢速连接攻击、连接耗尽攻击、Loic、Hoic、Slowloris、 Pyloris、Xoic等慢速攻击。
- Web应用层DDoS攻击：包括HTTP Get Flood、HTTP Post Flood、CC等攻击。

案例：GitHub遭受DDoS攻击

- 2018年美国东部时间 2 月 28 日，GitHub 在一瞬间遭到高达 1.35Tbps 的带宽攻击。这次 DDoS 攻击几乎可以堪称是互联网有史以来规模最大、威力最大的 DDoS 攻击了。
- 在 GitHub 遭到攻击后，事件并没有停歇，仅仅一周后，DDoS 攻击又开始对 Google、亚马逊甚至 Pornhub 等网站进行了 DDoS 攻击。后续的 DDoS 攻击带宽最高也达到了 1Tbps。



https://www.wired.com/story/github-ddos-memcached

如何防范DDoS攻击?

- **一个类比的例子**：我开了一家有五十个座位的重庆火锅店，由于用料上等，童叟无欺。平时门庭若市，生意特别红火，而对面二狗家的火锅店却无人问津。二狗为了对付我，想了一个办法，叫了五十个人来我的火锅店坐着却不点菜，让别的客人无法吃饭。
- **高防服务器**：高防服务器主要是指能独立硬防御 50Gbps 以上的服务器，能够帮助网站拒绝服务攻击，定期扫描网络主节点等；重庆火锅店增加了两名保安，这两名保安可以让保护店铺不受流氓骚扰，并且还会定期在店铺周围巡逻防止流氓骚扰。
- **黑名单**：面对火锅店里面的流氓，我一怒之下将他们拍照入档，并禁止他们踏入店铺，但是有的时候遇到长得像的人也会禁止他进入店铺。这个就是设置黑名单，此方法秉承的就是“错杀一千，也不放一百”的原则，会封锁正常流量，影响到正常业务。

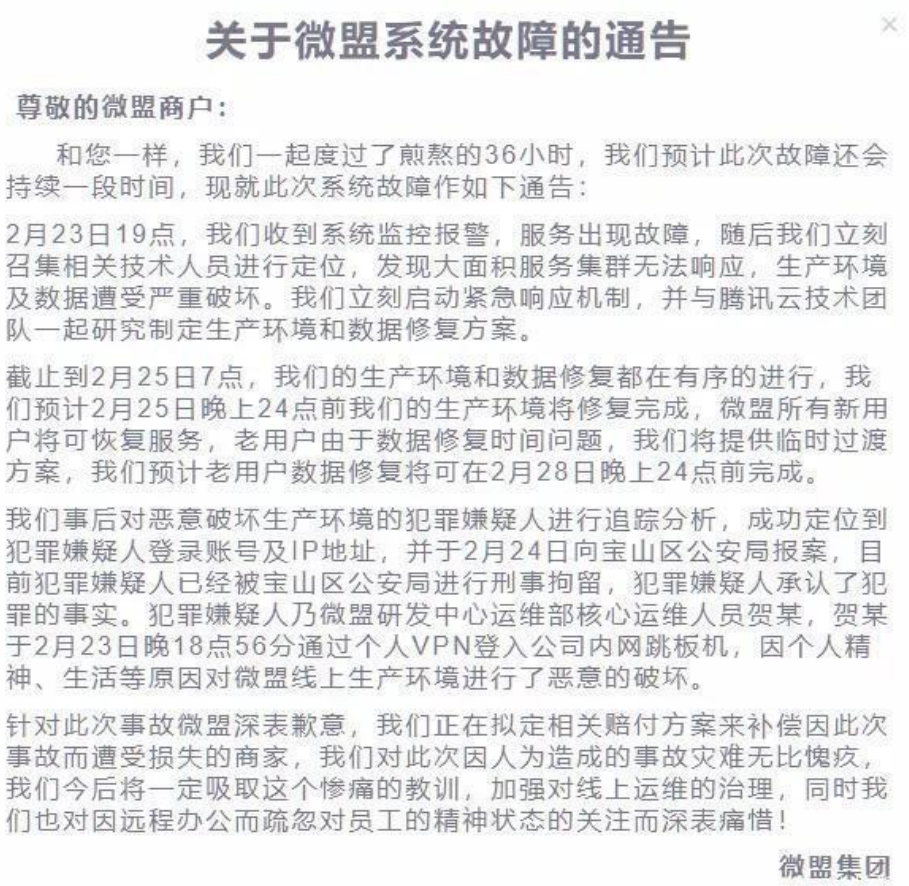
- **DDoS清洗：**DDoS 清洗会对用户请求数据进行实时监控，及时发现DOS攻击等异常流量，在不影响正常业务开展的情况下清洗掉这些异常流量。DDos 清洗，就是我发现客人进店几分钟以后，但是一直不点餐，我就把他踢出店里。
- **CDN加速：**CDN的全称是Content Delivery Network，即内容分发网络。CDN是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。在现实中，CDN服务将网站访问流量分配到了各个节点中，这样一方面隐藏网站的真实 IP，另一方面即使遭遇 DDoS 攻击，也可以将流量分散到各个节点中，防止源站崩溃。为了减少流氓骚扰，我干脆将火锅店开到了线上，承接外卖服务，这样流氓找不到店在哪里，也耍不来流氓了。

（4）还有很多种

- 蠕虫病毒
- 浏览器攻击
- 恶意软件攻击
- 跨站点脚本XSS
- 端口扫描
- 内部人员攻击

案例：堡垒都是从内部攻破的

- 2020年2 月 23 日 19:00 左右，微盟收到系统监控警报，获悉 SaaS 业务服务出现故障，生产环境及数据遭受严重破坏。
- 经排查，犯罪嫌疑人是微盟研发中心运维部核心运维人员贺某，贺某于 2 月 23 日晚 18 点 56 分通过个人 VPN 登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意的破坏，目前已被拘留。
- 这一事件给微盟集团带来的损失非常惨重，从 2 月 24 日至 2 月 25 日员工恶意破坏事件的一天时间内，微盟集团市值蒸发了约 9.63 亿港元。



关于微盟系统故障的通告

尊敬的微盟商户：

和您一样，我们一起度过了煎熬的36小时，我们预计此次故障还会持续一段时间，现就此次系统故障作如下通告：

2月23日19点，我们收到系统监控报警，服务出现故障，随后我们立刻召集相关技术人员进行定位，发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。我们立刻启动紧急响应机制，并与腾讯云技术团队一起研究制定生产环境和数据修复方案。

截止到2月25日7点，我们的生产环境和数据修复都在有序的进行，我们预计2月25日晚上24点前我们的生产环境将修复完成，微盟所有新用户将可恢复服务，老用户由于数据修复时间问题，我们将提供临时过渡方案，我们预计老用户数据修复将可在2月28日晚上24点前完成。

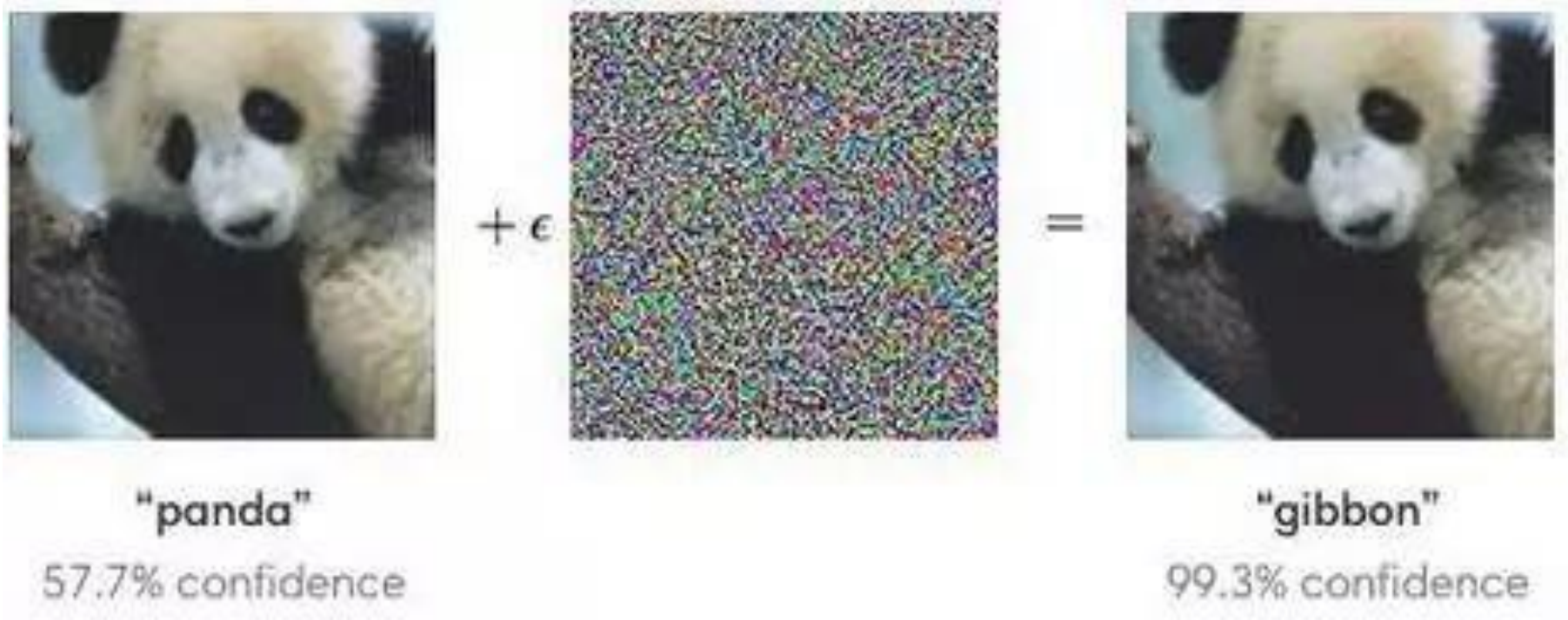
我们事后对恶意破坏生产环境的犯罪嫌疑人进行追踪分析，成功定位到犯罪嫌疑人登录账号及IP地址，并于2月24日向宝山区公安局报案，目前犯罪嫌疑人已经被宝山区公安局进行刑事拘留，犯罪嫌疑人承认了犯罪的事实。犯罪嫌疑人乃微盟研发中心运维部核心运维人员贺某，贺某于2月23日晚18点56分通过个人VPN登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意的破坏。

针对此次事故微盟深表歉意，我们正在拟定相关赔付方案来补偿因此次事故而遭受损失的商家，我们对此次因人为造成的事故灾难无比愧疚，我们今后将一定吸取这个惨痛的教训，加强对线上运维的治理，同时我们也对因远程办公而疏忽对员工的精神状态的关注而深表痛惜！

微盟集团

（5）AI安全性——GAN

- 基于深度神经网络模型的系统，很容易被欺骗愚弄。 如图所示，对于一张熊猫的照片，加上人为设计的微小噪声之后，人眼是对两张图片看不出分别的，计算机却会以99.3%的概率将其错判为长臂猿。



- 对于一些人为生成的在人眼看来毫无意义的噪声或者纹理，计算机也会以极高的概率将其分为某种类别。上述由恶意的攻击者故意设计生成的以欺骗人工智能系统的样本被称为对抗样本（adversarial samples）。
- 例如，对于可以自动识别交通标志的无人驾驶系统，攻击者生成一个禁止通行标志的对抗样本，自动识别系统会将其误判为是可以通行的标志。当自动驾驶系统和人类驾驶员同时驾车行驶时，这足以造成灾难性的后果。（两者从肉眼看基本是无差别的。）

AI隐身

比利时天主教鲁汶大学的学生展示了AI时代的「隐身术」，只要将一张利用对抗网络生成的图像放在身上，AI系统就无法检测出这是一个人。论文arxiv.org/pdf/1904.08653...

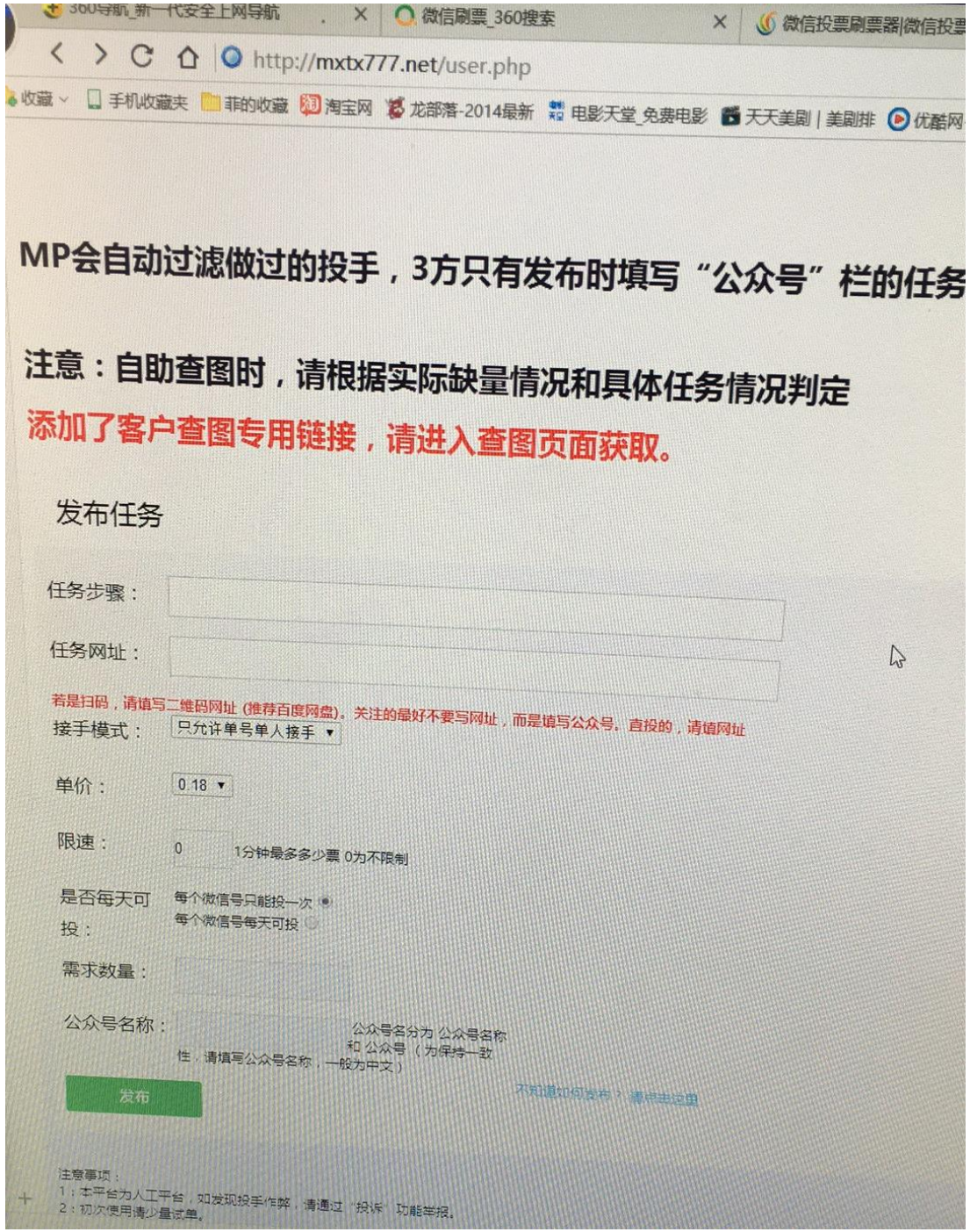
3. 钻系统的漏洞

1. 薅羊毛

- 引例
- 2018年7月，快手系统升级中，提现系统出现了一个小小的bug。订单失败后提现黄钻返回快手用户账户，但支付网关没有停止转账请求，还在不断尝试。在此期间，如果对应微信账号开通实名认证，则资金将从快手企业账户划拨至个人微信账户，用户将在未扣除黄钻情况下获得提现。利用这个漏洞，27人在24天内，从“快手”827名用户的4629笔订单中盗刷672万元。
- 被告人谢某等人利用所掌控账户的直播功能，首先通过账户互相打赏将对应黄钻攒至2000元，而后关联未开通或已经注销微信实名认证的账户反复提交提现申请，并在短时间内开通微信实名认证，资金到达微信账户后，迅速通过所绑定的银行卡第二次转出、分配。
- 以此方式，一条租号、打赏、提现、转账、取钱的黑色链条快速形成、蔓延，直到快手公司进行财务数据汇总，发现用户提现金额和个税数据不匹配、提现金额明显异常后，这一漏洞方被修正。
- 法院查明，2018年7月21日1时开始，到2018年8月2日22时，12天里，仅谢某一人就通过上述方式收购10组他人账号，累计套取资金125万余元。谢某最终被处罚金十一万元人民币，责令退赔经济损失一百二十五万余元人民币。同时，谢某与其他26人，因盗窃罪分获11年半到1年1个月不等的有期徒刑。

- **网络漏洞形成的黑色产业链是司法打击的重点**
- “薅羊毛”是与电子商务伴生的互联网现象。“薅羊毛”行为按照轻重程度可以分为三类：
- （1）按照平台优惠规则、偶尔利用平台漏洞获取优惠自用的普通用户；
- （2）利用平台优惠规则疏漏、借助信息及技术优势攫取优惠后进行二次转卖、变现的“羊毛党”；
- （3）利用系统漏洞恶意牟利的黑灰产链条。上文的快手盗刷案，即属于第三种。
- 对于第一类行为，使用者属于正常消费行为，在法律、商业规则及市场规律范围内无须担心。事实上，这个层面的消费者的注意力应该集中在自身权利维护，尤其是在损失是由平台自身过错造成，消费者并无任何欺诈等心态的情况下。对此，不同平台反映不一，如去哪儿网、东航因系统失误而出现的超低价机票订单，最终宣布正常出票；但万豪酒店出现酒店订单错误，酒店最终取消已订房用户订单，平台赔偿 5000积分。

- **网络漏洞形成的黑色产业链是司法打击的重点**
- 对于第二类专业“羊毛党”，明显恶意违法平台规则及利用系统漏洞的，在民事法律关系上属不当得利，受损害平台可以请求返还，在刑事法律评价上则相对暧昧，无法一概而论，但其中具有主观恶性，违法所得数额较大或影响较大的，同样构成刑事犯罪。
- 对于第三类利用系统漏洞恶意牟利的黑灰产链条，是目前的打击重点，本案中呈现出一个黑产新趋势：非法支付渠道向普通个人账号转移。
- 一般来说网络黑产的供给链可以划分为物料、流量和支付三大要件，以恶意注册账户为主供养物料，通过虚拟商品交易作为变现的主要渠道；而在羊毛灰产中则细化为卡商负责注册平台账号-网络黑客人员负责买卖“秒杀软件”-“羊毛党”负责在平台使用-收货端负责在二级市场变现。
- 但随着各个互联网平台尤其是几家互联网巨头对于恶意注册的联合打击，技术壁垒日益垒高，“养号”成本日益增高。于是黑产将目标锚定普通个人账号，如小许及胡某等人提供的账号，该种账号属正常账号，在技术上无法识别；这虽然在打击犯罪上提供了便利，但也对溯源上游犯罪带来挑战。


360导航_新一代安全上网导航
微信刷票_360搜索
微信投票刷票器|微信投票
http://mxtx777.net/user.php
收藏
手机收藏夹
菲的收藏
淘宝网
龙部落-2014最新
电影天堂_免费电影
天天美剧 | 美剧排
优酷网
MP会自动过滤做过的投手，3方只有发布时填写“公众号”栏的任务
注意：自助查图时，请根据实际缺量情况和具体任务情况判定
添加了客户查图专用链接，请进入查图页面获取。
发布任务
任务步骤：
任务网址：
若是扫码，请填写二维码网址 (推荐百度网盘)。关注的最好不要写网址，而是填写公众号。直投的，请填网址
接手模式：
只允许单号单人接手
单价：
0.18
限速：
0
1分钟最多多少票 0为不限制
是否每天可投：
每个微信号只能投一次
每个微信号每天可投
需求数量：
公众号名称：
公众号名分为 公众号名称 和 公众号（为保持一致性，请填写公众号名称，一般为中文）
发布
不知道如何发布？请点击这里
注意事项：
1：本平台为人工平台，如发现投手作弊，请通过“投诉”功能举报。
2：初次使用请少量试单。

2. 优惠券漏洞

- **拼多多“优惠券漏洞”**
- 2019年开年拼多多“年货节”大促，期间有大批量平台正常发放的优惠券被消耗。至20日上午9点，遭盗取优惠券和正常优惠券的总和突破平台预设阈值，系统监控到异常并自动报警后，拼多多在第一时间修复了相关漏洞。
- 拼多多表示，黑灰产团伙所利用的“优惠券漏洞”盗取的相关优惠券，系拼多多此前与一档电视节目（江苏卫视《非诚勿扰》）开展合作时，因节目录制需要特殊生成的优惠券类型，仅供现场嘉宾使用。
- 除此之外，此种类型优惠券，从未在任何时候、以任何方式出现在平台正常的线上促销活动当中，甚至从未有任何线上入口，这与“某航空公司在官网由于误操作发放低价机票”等事件具有根本性质差异。
- 而该事件中的相关优惠券，均系黑灰产团伙通过非正常途径生成的二维码扫码后获得，该二维码多流传于社交平台相关黑灰产群。拼多多从未针对该类型优惠券生成任何二维码，更从未在APP及小程序中展示过此类优惠券相关信息及二维码。

- **拼多多“优惠券漏洞”**
- 拼多多透露，黑灰产通过该非正常途径生成的二维码，原本每个认证信息的用户可且仅可领取一张无门槛100元优惠券，而非此前网络流传的单个ID可以“无限领取”
- 因此，有黑灰产团伙通过“养猫池”（用手机卡蓄养大量虚拟账号）等不法手段，实现N张手机黑卡同时作业，批量盗取该种优惠券，并通过手机话费、Q币等虚拟充值的方式，试图在短时间内迅速转移此类不当所得。
- 拼多多风控团队负责人表示，黑灰产团伙在盗取金额巨大的优惠券并转移其不当所得后，期望达成“法不责众”的效果，迅速通过网络和社交群将二维码分享出去，诱导一些普通消费者跟风扫码，并在社交平台和群内编造“拼多多平台发券损失200亿等谣言”，以希望达到逃避刑责、混淆视听的结果。

3. 刷好评

- **Steam下架“视趣互动科技”所有游戏**
- 2017年，V社将两款名为《The Dawn:First War》和《Last Stand》游戏都从Steam移除了，原因是发现开发者利用漏洞来刷好评。
- 据悉，有一些开发商会试图通过刷好评的行为提高游戏的评分，通过这样的不正当手段来吸引玩家下载。其主要原因是很多消费者在购买游戏时，除了开发商的介绍、宣传片和截图外，大家都习惯于查看一下社区的评价，如果好，才会选择购买。
- 作为世界最大的游戏发行平台之一，Steam成为了许多VR游戏厂商的首选。然而，“刷好评”导致部分玩家因这些不负责任的评价而被误导，是玩家对VR游戏失去信任，影响了整个VR游戏行业的发展。

4. 将系统用于违法业务

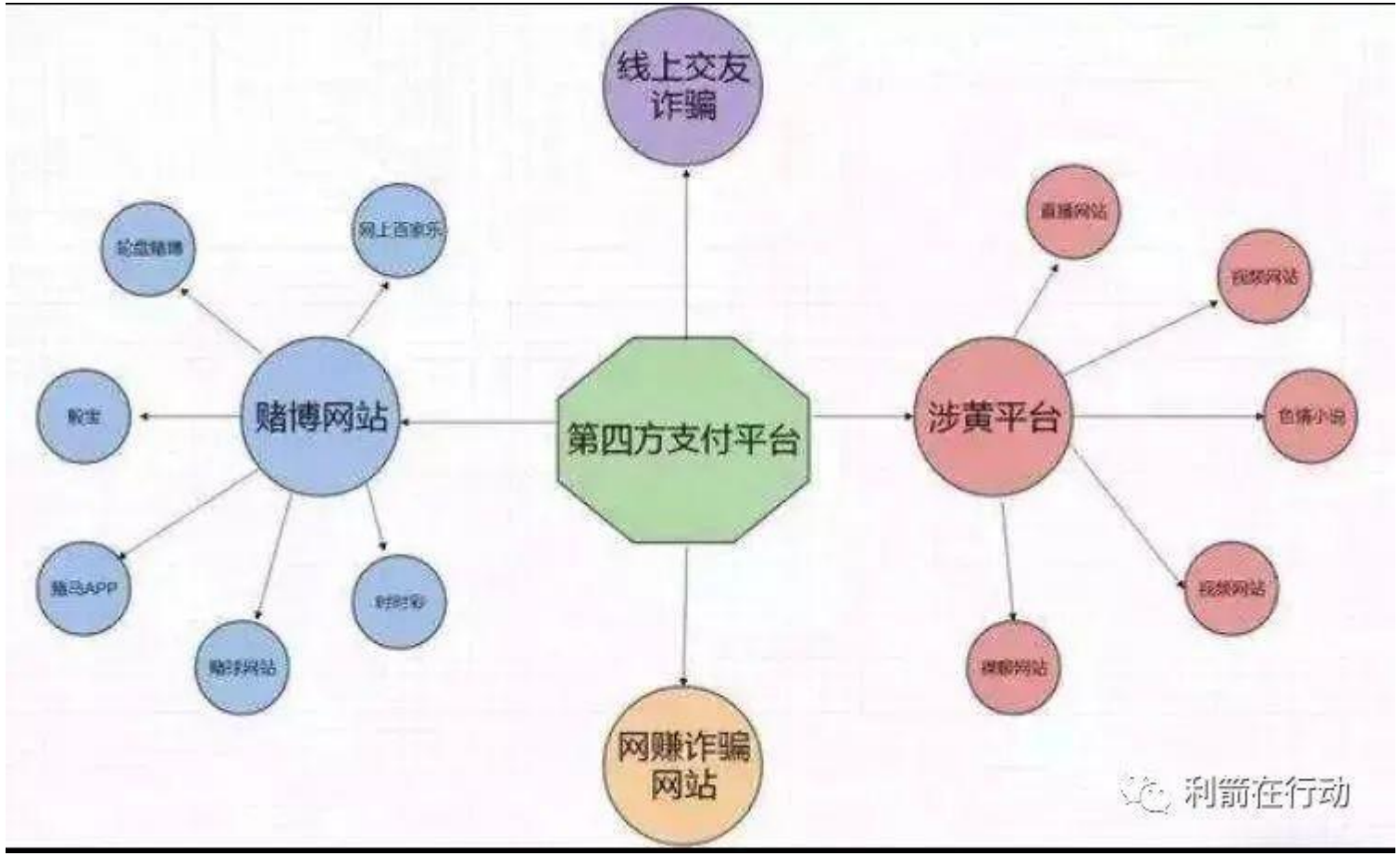
1. 灰色产业链

- **灰色产业：**介于正当行业（白）和不正当行业（黑）之间的不合理但又客观存在的产业。
- 简单地说，灰色产业就是和法律打擦边球，暴利的项目或者产业。
- **互联网灰色产业：**
- **（1）灰色软件形成的灰色产业**
- 对于灰色软件，或者称之为恶意软件、流氓软件，它们都有一些共同特征：用户未授权、不知情即自行安装，具备一定的实用价值，但对用户的软件硬件及个人信息带来潜在威胁，不易卸载等。灰色软件大致经历了恶意网页代码、插件推广、软件捆绑和流氓软件病毒化四个阶段。目前，灰色软件主要有几类：广告软件、间谍软件、行为记录软件和恶意共享软件等。
- **（2）网络水军形成的灰色产业**
- 经过不断发展，网络水军进一步发展，形成数量众多更高级形式的网络公关公司。这些公关公司可以组织成千上万的"水军"炒作话题、引导舆论，已成为一个操作流程非常成熟的行业。比如在网上看到的消息、新闻，特别是论坛里的很多能调动人气热点帖、热点话题、"网络红人" 有很多可能是不真实的，是公关公司策划和操纵的。

- **（3）部分合法公司参与灰色产业的现象**
- 众多合法公司往往也以各种形式参与到互联网灰色产业中来，而且正是这些合法企业的参与，使灰色产业发展壮大，声势浩大。
- 例如某著名搜索引擎服务商利用其搜索引擎的有利优势，以竞价排名方式盈利，遭到社会各界质疑。另一方面，它可以根据需要对搜索结果进行过滤，从而为客户屏蔽某些不利信息而获利。网络公司利用其强大的资源聚集能力， 为客户在网络上发布软文，导向舆论、混淆视听甚至于控制不利信息等。在淘宝这类交易网站，信誉系统对于买家而言，很大程度上是其购买的一个重要参考依据， 也正是看中了这一点，透过网络，有组织的操纵信誉评价系统的现象非常严重，并形成了完整的灰色产业链。

2. 四方支付

- **第四方支付**
- 近年来，支付宝、微信等“第三方支付”因其高效便捷而风靡全国。不过，支付宝、微信财付通等第三方平台监管严格，非法网站无法接入，一些非法的“第四方支付平台”应运而生，它们为赌博、私彩等从事违法犯罪的网络平台或贩毒、诈骗等犯罪提供资金支付结算通道，从中获取高额回报。
- 第四方支付，又可称之为“融合支付”或“一码支付”，是一种通过技术手段将银行、第三方支付等多种支付服务方式融合为一体的综合性支付服务，常见的聚合支付产品有聚合扫码、智能POS、扫码枪、扫码盒子等。第四方支付最初作为第三方支付外包服务商的角色出现，并随着移动支付规模爆发式增长而快速发展。
- **案例**
- 2018年年底至2019年8月，刘某某等人为获取巨额非法利润，利用注册空壳公司，以公转私、套取现金的形式，非法为他人提供单位银行结算账户套现或者单位银行结算账户转个人账户服务，为“大满贯”赌博平台等提供掩饰。
- 易某等人从全国各地办理数万张物联网卡，然后用物联网手机号向某通讯公司申请手机充值卡卡密，赌客在“大满贯”等上充值并完成支付后，会通过刘某某团伙建立的“华荣聚富”支付结算系统进行流转，由易某等收集卡密，进行“洗钱”。“洗白”的资金由刘某某团伙进行代付，给赌博人员提现。刘某某等人建立的具有代付结算功能的平台，上游负责对接商户资金流入，下游对接商户资金流出。



- 刘某某等人从事的非法支付结算是一种新型犯罪，是犯罪分子在未经许可的情况下，依托网络进行的非法经营行为，在整个资金转移过程中，它起着中介作用。而为违法犯罪提供非法支付结算业务搭建的支付平台被称作“第四方支付平台”。这种通道未获得国家支付结算许可，违反国家支付结算制度，依托支付宝、财付通等正规第三方支付平台，通过大量注册商户或个人账户非法搭建形成。
- 由于“第四方支付”平台没有支付许可牌照且由个人组建，资金安全没有保障。

2. 两卡犯罪

- **“两卡”犯罪**
- 是指非法出租、出售、购买“两卡”的违法犯罪活动。所谓“两卡”是指手机卡、银行卡，其中，银行卡既包括个人银行卡、对公账户、结算卡，同时还包括非银行支付机构账户，即大众常用的微信、支付宝等第三方支付。
- 2020年8月，某学院在校学生刘某学休学后，为尽快挣钱，主动加入贩卡团伙成为“收卡人”，期间收购、贩卖手机卡871张，获利人民币1.5万余元；某高校或中专在校学生吴某豪等9人，向诈骗团伙出售9套银行卡资料。在明知本人银行账户内转入资金系他人犯罪所得的情况下，仍分别转移诈骗资金2.45万元至29.16万元不等。
- 最高人民检察院、教育部日前联合印发一批在校学生涉“两卡”犯罪典型案例，进一步深刻揭示电信网络诈骗犯罪危害，加强警示教育，努力为在校学生营造更加良好的成长成才环境。

3. 呼叫中心诈骗

- **呼叫中心诈骗**
- VoIP用户可以得到呼叫者的ID字段，它可以被设置为任何他们所想要的。这对那些诈骗犯来说是一个关键的优势，因为他们不需要很多技术来完成这项工作。诈骗犯罪者已经开发了软件来重置PINs和进入帐户和IVR系统。。
- 呼叫中心是一个利润丰厚的诈骗活动渠道。每月有超过1000亿的呼叫中心电话通话。诈骗者意识到这一点，并通过对电话系统的攻击渗透到客户账户中。有三种主要类型的呼叫中心诈骗：
- （1）帐户接管--诈骗者冒充合法客户，通过呼叫中心座席改变账户的联系信息或PIN号码。
- （2） 信用卡诈骗--犯罪分子用偷来的信用卡信息在电话上发号施令。通常，订单在欺诈被发现之前被处理和发送。
- （3）数据泄露--犯罪分子利用电话渠道进行侦察。攻击者发现，电话渠道是企业和消费者的薄弱环节。

4. CaaS

- **犯罪软件即服务或网络犯罪及服务（Crimeware-as-a-Service，CaaS）**
- 指在网络犯罪生态系统中技术人员向其他网络犯罪分子提供产品和服务的行为。这种模式为网络犯罪集团的攻击活动提供了便利，即使技术上缺乏经验的犯罪分子和高级威胁行为者也能迅速实施复杂的攻击，而不需要借助先进的技术。
- CaaS降低了威胁攻击者发动网络攻击的门槛，对于高级威胁攻击者来说是一个绝佳的选择。犯罪软件即服务的模式使得犯罪很难归咎于某个特定的个人，因为犯罪手段的实施和攻击工具都是由多个网络攻击者共享的。
- 在CaaS框架下，最受欢迎的产品包括恶意软件、勒索软件、网络钓鱼工具，以及基础设施的控制权限。这些服务大多数特点是易于用户使用，而且有强烈的客户导向。它们通常有方便用户进行管理的控制台或仪表盘。
- 犯罪活动的成本由所有“客户”共同来分担，这得益于一种基于订阅或统一费率收费的模式，使得网络犯罪服务变得更加方便和有吸引力。在这种情况下，网络攻击服务提供商可以增加他们的收入，而客户则可以从合理减少管理非法业务上所花费的费用中获益。

- **犯罪软件即服务或网络犯罪及服务（Crimeware-as-a-Service，CaaS）**
- 网络犯罪威胁领域的专业化程度正在提高，这使得CaaS模式非常危险。一些犯罪组织特别注重向其他犯罪团伙提供犯罪服务和产品，而不是直接以其手段针对用户和组织。
- 在广泛使用的CaaS解决方案的背景下，不太懂技术的网络罪犯有所增加。
- CaaS服务在网络犯罪论坛和暗网市场中相当容易找到，并且具有很大的影响力。犯罪分子只需用比特币下单付款，就可以租用一个僵尸网络。然后，全球数千台被感染的机器就可以被雇佣于从事各种非法活动，如分发恶意软件、发起DDoS攻击或发送垃圾邮件。
- 最近几个月，勒索软件即服务模式(RaaS)的普及使得勒索软件攻击数量快速上升。
- RaaS以云端订阅的模式可以提供给任何能够支付订阅费的人。另一方面，一些勒索软件运营商不收取订阅费，而是采用“联属”模式，即他们收到联属公司向受害者勒索的所有赎金后，自己保留一定的比例作为佣金，然后将其余部分转给联属公司。

谢谢！

Thank you for your attention.

liuyuewen@xjtu.edu.cn