



互联网信息安全意识培训

1

信息安全概述

2

个人安全意识

3

办公安全意识



信息安全概述



什么是信息安全？



**信息安全就像刹车，
防止车祸的发生**

信息安全三要素

确保信息不会泄露给非授权个人或机构

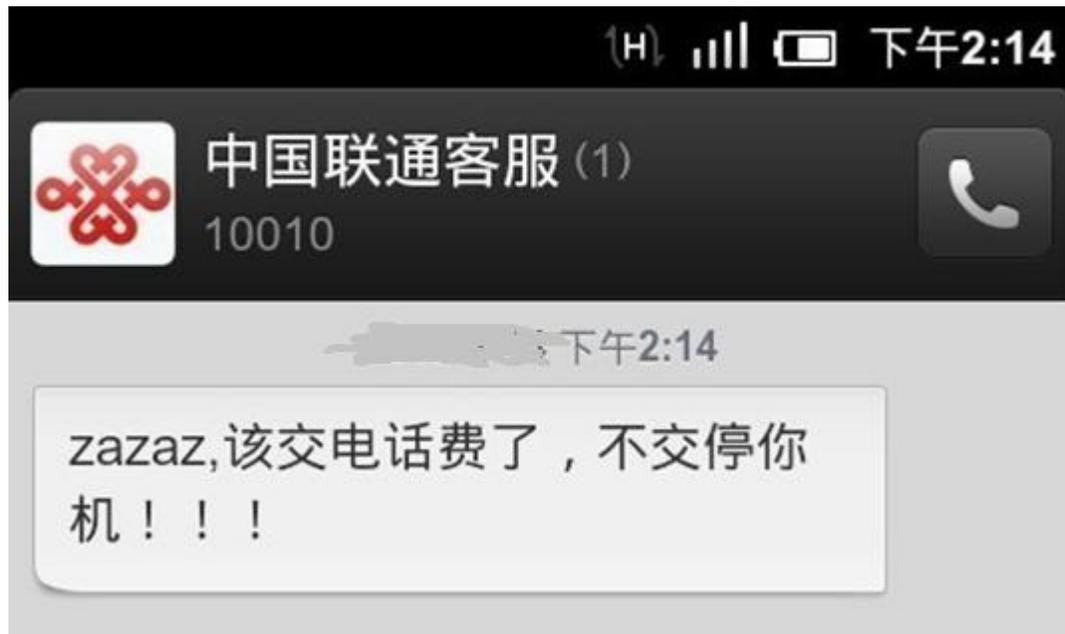


确保信息或资源可以正常使用，不会被异常拒绝

确保信息不会被篡改



信息安全—完整性



信息安全—可用性



5月19日全国六省断网 十万网站无法访问事件追踪

导读：2009年5月19日，中国出现大范围网络故障。江苏、河北、山西、广西、浙江、天津、内蒙古、黑龙江、广东等省份均有网民反映上网遭遇故障，出现打不开网页等问题。

5月19日DNS大规模故障 域名服务商遭恶意肉鸡攻击

暴风就断网事件道歉 承认存在缺陷
北京暴风网络科技有限公司(以下简称暴风)发布了暴风公司关于断网事件向网民和新老用户的公开信，正式就这件事道歉，并称已正式完成报案程序。【全文】

- 独家采访万网技术副总：断网事件警醒运营商

名词解释
什么是DNS?
DNS是域名系统 (Domain Name Server) 的缩写，该系统用于命名组织到层次结构中计算机和网络服务。在Internet上域名与IP地址之间是一一对一(或者一对多)的，域名虽然便于人们记忆，但机器之间无法互相认识IP地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS就是进行域名解析的服务器。DNS 命名用户

友情提示
系统忙，请您稍后再试。
您可能需要：[返回支付宝首页](#)

2015年5月27日，
支付宝断网事件



中国联通 4G 上午11:15 93%

推荐 热点 科技 体育 财经 电影

硬件 软件 互联网电商 人工智能 更多

网络不给力，点击屏幕重试

500

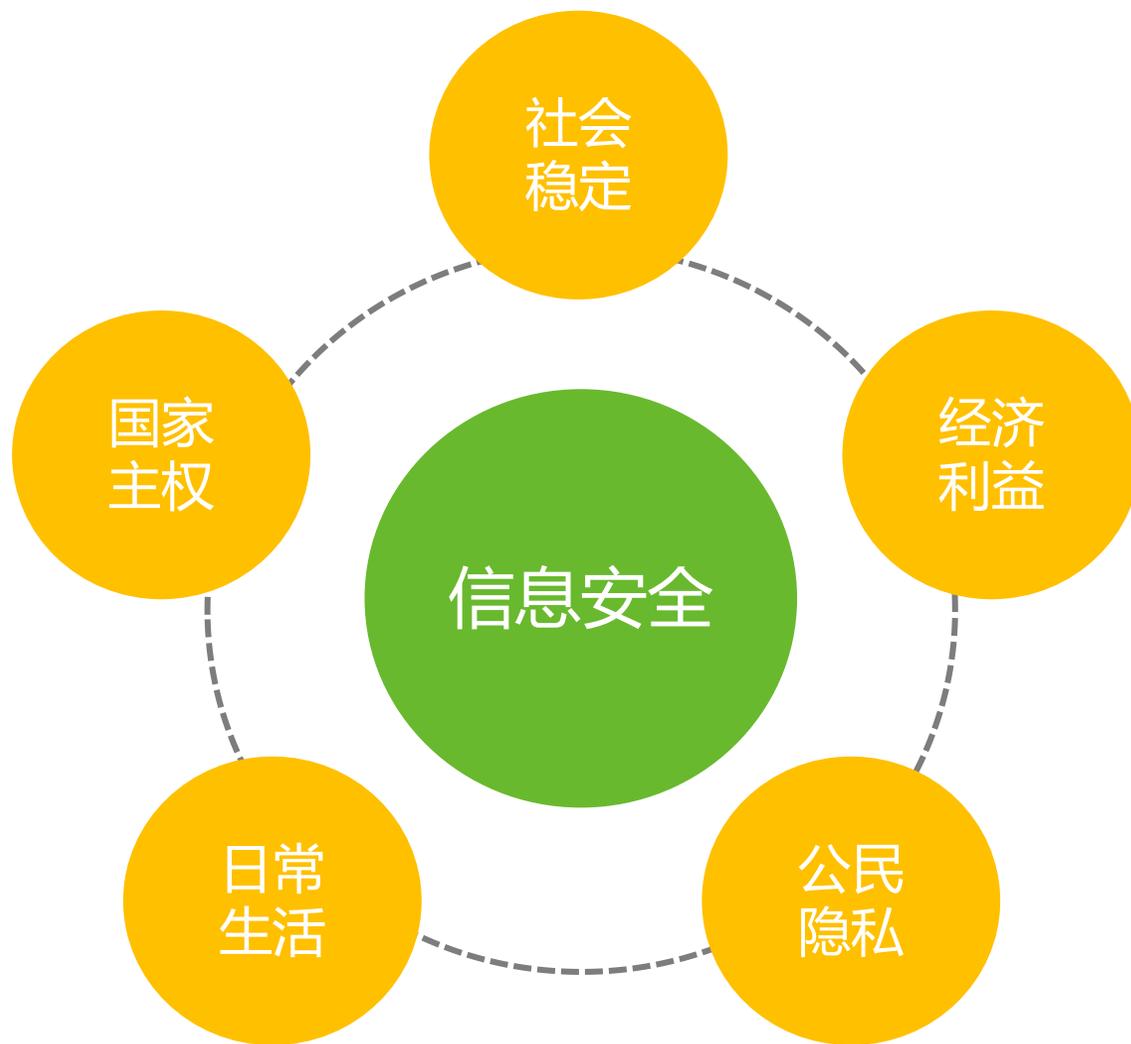
头条君找不到你想要的页面...
(HTTP 500内部服务器错误)

2017年1月 今日头条服务器
宕机，影响长达30分钟

504 Gateway Time-out

nginx/1.9.10

信息安全影响范围



国内信息安全现状



网络信息安全已纳入国家战略



大量网络安全事件发生



新兴技术应用带来的安全风险





常见安全隐患-钓鱼网站





常见安全隐患-钓鱼短信

中国移动 08:09 96%
信息 95555 详细信息

短信/彩信
昨天19:57

招商银行紧急通知：您的手机银行将已次日失效，请速登入招行手机网 wap.cmbc.com 升级激活，给您带来不便敬请谅解！【招商银行】

The screenshot shows a mobile application interface for China Merchants Bank. At the top, there is a blue header with the bank's logo and name. Below the header, there are three tabs: '一卡通', '信用卡', and '一网通'. The main content area contains several input fields: '卡号' (Card Number) with a placeholder '请输入您的卡号', '查询密码' (Query Password) with a placeholder '请输入查询密码', and '银行预留手机' (Bank Reserve Mobile) with a placeholder '请输入银行预留手机号'. There is also a '附加码' (Additional Code) field with a refresh button and the value '8429'. A '记住卡号' (Remember Card Number) toggle switch is present. A large blue button labeled '下一步' (Next Step) is at the bottom of the form. Below the button is a '业务助手' (Business Assistant) link. At the very bottom, there is a promotional banner for '手机转账0费用, 享3年!' (Mobile Transfer 0 Fee, Enjoy 3 Years!) with a '下载' (Download) button. On the right side of the page, there is a white box with a progress bar showing '8%' and the text '系统正在收录您的个人数据, 请勿关闭页面.' (System is collecting your personal data, please do not close the page). At the bottom right, there is a footer with the text '二十四小时服务热线: 95555' (24-hour service hotline: 95555) and '© 2014 招商银行 版权所有 未经许可 不得转载' (© 2014 China Merchants Bank. All rights reserved. No unauthorized reproduction or distribution).

常见安全隐患-朋友圈隐私泄露



- 晒娃
- 购物
- 旅游
- 美食
- 炫富

常见安全隐患-随意连接公共WIFI



黑客伪装成常用公共wifi，例如：cmcc-Starbucks

手机自动连接上后，黑客能得到你的手机型号、登录历史、设备使用者名称、语言设置和设备操作系统版本。

如果你在此时登录了你的邮箱或支付宝等，那么这些信息很容易就会被黑客获取。

更加恐怖的是，黑客还可以转移你访问的地址，他可以让你登录伪造的银行网址等，这样的网站完全受黑客控制，但你却一无所知。

常见安全隐患-勒索病毒邮件

攻击流程:



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95 09 00 Next >>



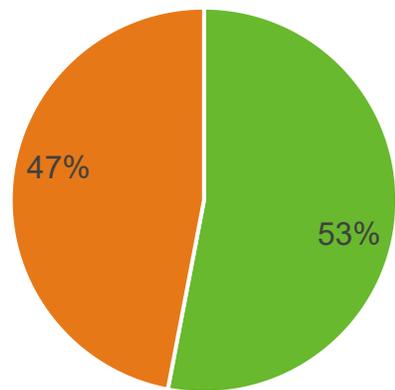
个人安全意识



▶▶ 中国人愿意用隐私换取便利---李彦宏

- 2017年5月31日,《南方都市报》与中国政法大学传播法研究中心联合发布《互联网企业隐私政策透明报告》。对1000家常用网站、APP的用户信息保护政策透明度进行排名,结果显示,测评的生活服务、休闲娱乐、医疗健康等各个领域1000家平台中,超过50%的网站与APP评分为“低”级别,令人担忧。**中国人对隐私问题更加开放,或者说没有那么敏感,如果要用隐私来交换便捷性或者效率的话,很多情况下中国用户是愿意这么做的。**

你愿意提供个人信息以获得更便利的服务吗?



■ 愿意 ■ 不愿意



▶▶ 神奇的“读心”大师



二维码安全隐患



张先生是做家具定制生意的，近几年生意越做越大，他也开了一家网上旗舰店，双十一期间生意特别好。

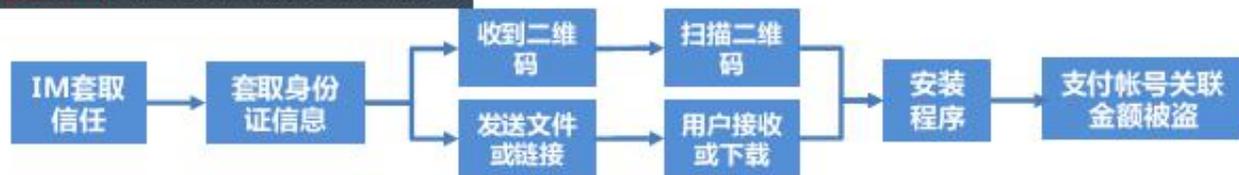
“前几天，有个人说他家里要装修，想定制些家具。那个人就和其他前来咨询的客人一样，没什么特别。”张先生每次回想这个事情，都特别懊悔。

“只是聊着聊着，那个买家突然说，他在外面，手机流量有限发不了那么多图，让我**扫描一个二维码**，下载后可以看到他想要的家具的图片和尺寸。”张先生说，“现在都流行扫一下二维码，我之前扫描过，很方便，就拿手机扫了一下。但是扫描后，我啥也没看到。”

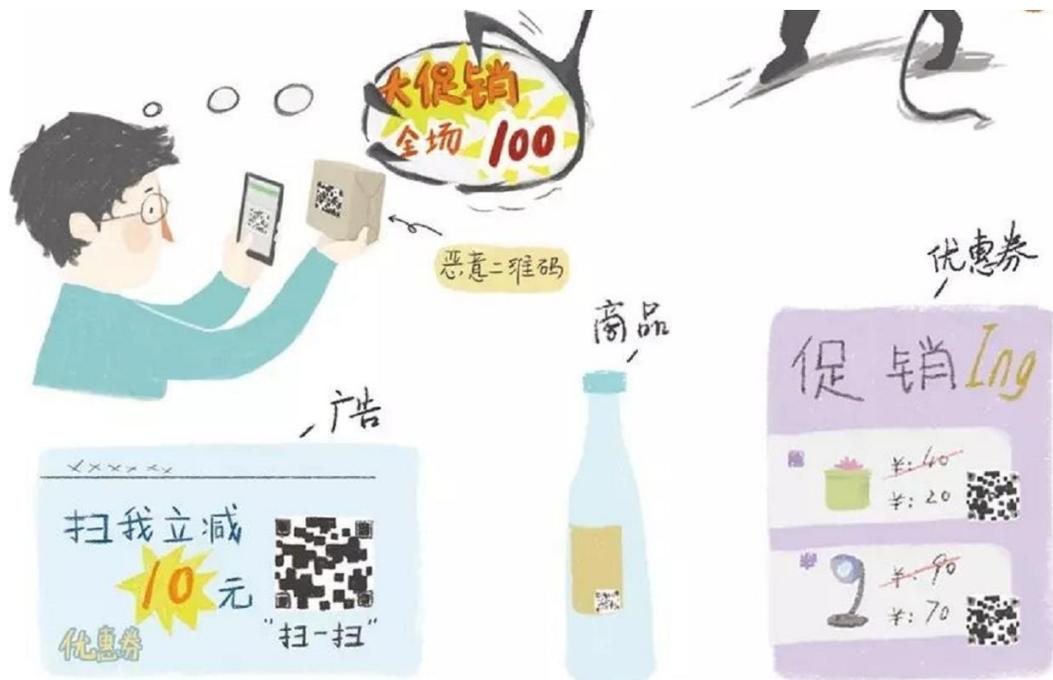
“后来我又和买家沟通了一会，他说先付些订金，问我要了姓名、身份证、银行卡、手机号等信息，说晚上回到家再汇款就下线了。”

晚上，张先生登录网银，看看买家的订金到账没有，却震惊地发现**银行卡内少了好几万**。张先生马上意识到自己被盗了，赶紧冻结了银行卡并向警方报案。

共同案情回放：



二维码安全隐患



虚假“优惠促销”

伪造付款二维码



假

假



假

二维码骗钱原理还原



不要轻信“二维码”！

个人信息安全概述

01 手机安全

02 社交安全

03 WIFI安全

04 个人安全防护

手机安全-系统及应用安全

◆ 操作系统不要越狱

◆ 采用指纹解锁

◆ 在安装手机软件时选择正规的软件市场下载安装

◆ 安装APP之前阅读隐私条例

◆ 及时安装系统和应用更新



手机安全-安全使用习惯

- ◆ 不要轻易的扫二维码
- ◆ 不要把手机连接到公共计算机上
- ◆ 不要使用公共充电器
- ◆ 借助第三方软件来保证手机的安全
- ◆ 不要把敏感信息存储在手机中
- ◆ 经常备份手机中的重要文件



社交安全-微信朋友圈



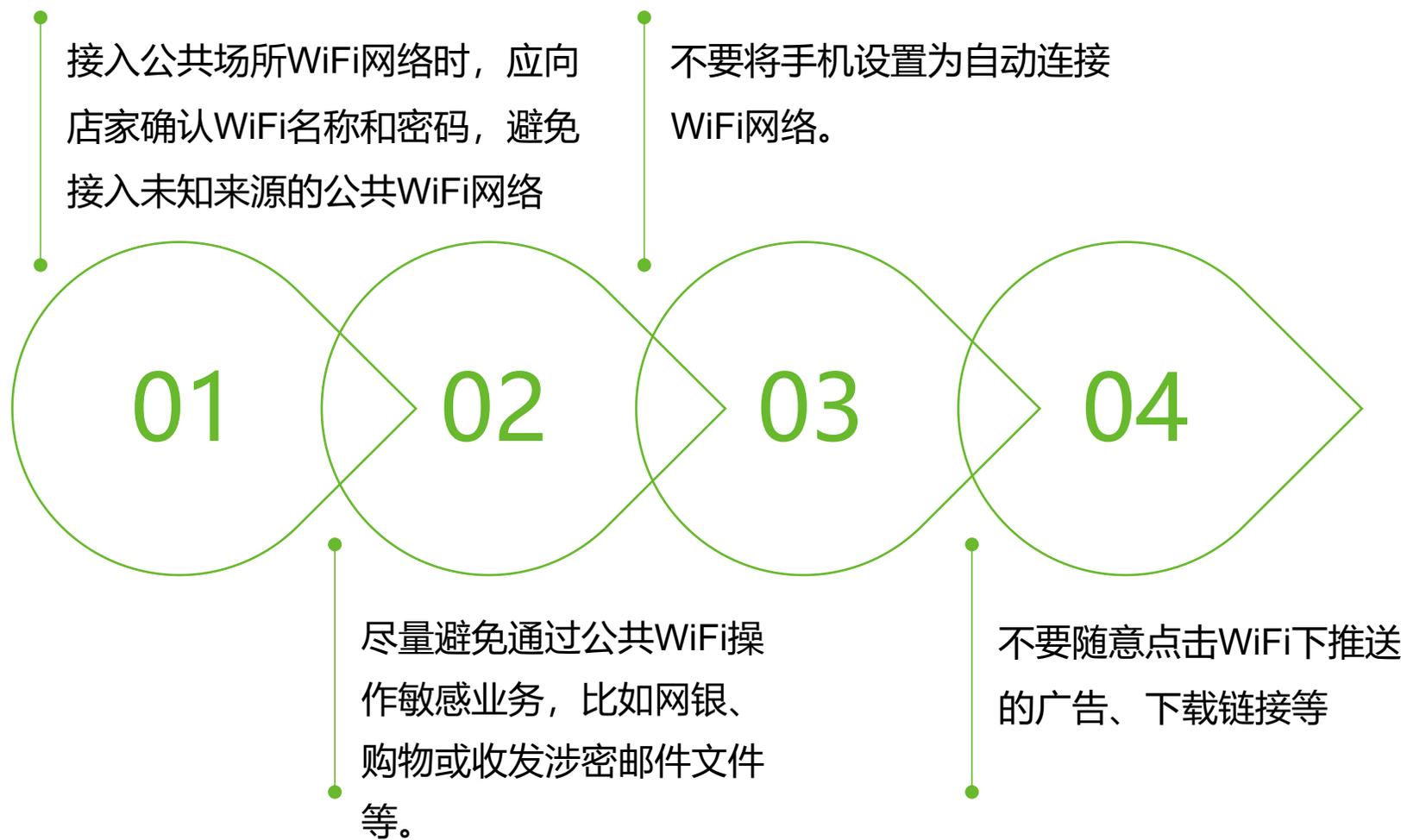
- 家人照片
- 地址
- 车牌号
- 贵重物品
- 行程信息
- 位置信息
- 个人身份信息

社交安全-微信安全使用习惯

- ◆ 给微信好友起个备注名
- ◆ 不要加陌生人为好友
- ◆ 与好友聊天过程中不要涉及敏感信息
- ◆ 借助第三方软件来保证手机的安全
- ◆ 不要把敏感信息存储在手机中



公共WiFi安全



个人安全防护-电脑安全

- ◆ 启用防火墙和防病毒功能
- ◆ 关闭USB设备自动播放
- ◆ 设置10分钟自动锁屏
- ◆ 不用的共享目录要及时关闭
- ◆ 使用非IE内核浏览器，谷歌、firefox等
- ◆ 设置强密码并定期修改
- ◆ 使用onedrive进行重要文件备份
- ◆ 使用BitLocker对磁盘进行加密



个人安全防护-支付安全

- ◆ 把磁条卡更换成芯片卡
- ◆ NFC信用卡使用卡套阻隔信号
- ◆ 设置刷卡限额
- ◆ 重点保护密码、磁道信息，卡片验证码（CVN和CVN2）、卡片有效期



签名

CVN
2

个人安全防护-四不提醒



- ✓ **不轻信**任何转账要求，务必电话确认。
- ✓ **不透露**短信验证码，发现手机收不到短信验证码马上送检。
- ✓ **不随意**点击链接，特别是聊天中发来的链接不要随意打开。
- ✓ **不在**非官方网站输入账号密码。



办公安全意识



安全小故事-1



安全小故事-2



▶▶ WANNACRY勒索蠕虫

- **时间：**2017年05月12日
- **目标：**未打MS17-010漏洞的windows系统
- **影响：**全球爆发了一系列勒索软件（Wannacry）的感染事件。国内大量企业遭到感染，多个高校的教育网受到感染，导致系统瘫痪。同时据英国广播电视台BBC报道，全球同一时间也爆发了多起勒索软件感染的事件，英国多家医院被感染，该勒索软件会加密被感染系统上的资料和数据，要求支付相应的赎金才会解密和恢复。包括俄罗斯，意大利，大部分欧洲国家，以及国内多所高校均被感染。



▶▶ GLOBEIMPOSTER变种勒索病毒

- **时间：**2017年05月
- **方式：**通过垃圾邮件、社交工程、渗透扫描、RDP爆破、恶意程序捆绑等方式进行传播
- **影响：**近期我们发现GlobeImposter3.0变种勒索病毒在国内较大范围内传播。通过分析本次捕获的最新样本并未发现样本具备其他新的传播方式。该家族加密的后缀名也随着变种的不同在进行变化，已经出现的变种加密后的后缀名有：.CHAK、.crypted!、.doc、.dream、.TRU E、..726、.Alcohol、.FREEMAN、.ALC0、.ALC02等，本次截获的最新本加密文件后会修改文件后缀名为“.Tiger4444”，该变种依旧是利用RSA+AES加密的方式，用户中招后无法对文件进行解密。



勒索软件

□ 什么是勒索软件？

- 对受害者电脑进行文件加密并进行勒索；
- 支付赎金也未必能恢复文件；

□ 勒索软件攻击流程

- 以钓鱼邮件的形式传播，邮件附件中往往包含经过伪装的恶意程序；受害者直接点击打开该恶意程序；（网页挂马、入侵、漏洞传播、文件感染）
- 恶意程序加密受害电脑上数据文件；
- 在受害者尝试使用文件时弹出勒索要求；



勒索软件 – 典型案例



Dear henry,

We would like to thank you for your recent order.

Order Status updated on: 21/03/2016

Your Customer ID: 618540

Your Order ID: 4CE92A76AD-M-2016

Invoice Number: 3514560

Delivery Note:

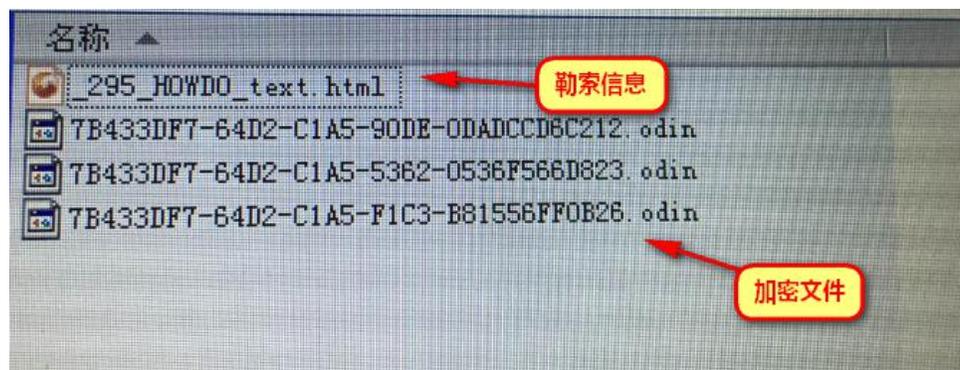
We received your order and payment on 17/03/2016

Your order details are attached.

Best regards,

Graig Macias

Key Account Manager



!!!重要資訊!!!!

您的所有檔已被RSA-2048 和AES-128暗碼進行了加密。

欲獲取更多關於RSA的資訊，請參閱：

<http://zh.wikipedia.org/wiki/RSA加密演算法>

<http://zh.wikipedia.org/wiki/高級加密標準>

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。

若要接收您的私人金鑰，請點擊以下其中一個連結：

1. <http://6dtxgqam4crv6rr6.tor2web.org/85C5EC6C40141199F>

2. <http://6dtxgqam4crv6rr6.onion.to/85C5EC6C40141199F>

3. <http://6dtxgqam4crv6rr6.onion.cab/85C5EC6C40141199F>

4. <http://6dtxgqam4crv6rr6.onion.link/85C5EC6C40141199F>

如果以上位址都無法打開，請按照以下步驟操作：

1. 下載並安裝洋葱瀏覽器 (Tor Browser) : <https://www.torproject.org/download/download-easy.ht>

2. 安裝成功後，運行瀏覽器，等待初始化。

3. 在位址欄輸入: 6dtxgqam4crv6rr6.onion/85C5EC6C40141199F

4. 按照網站上的說明進行操作。

! 您的個人識別ID: 85C5EC6C40141199F

▶▶ 勒索软件 – 如何防范

已经中招的用户暂时没有办法解密文件，可以将已加密的文件保管好等待互联网上安全人员研究并公开相关解密工具，不要寄希望于付费进行解密，在较大情况下都是骗局。

- 定期异地备份重要文件；
- 针对来历不明邮件中的附件，切勿随意打开；
- 在windows中设置显示文件扩展名，对于不熟悉的的文件扩展名，切勿双击打开；
- 针对office中的宏提示，不要进行点击运行。
- 设置高强度远程桌面登录密码并妥善保管；
- 安装防病毒软件并保持良好的病毒库升级习惯；
- 对内网安全域进行合理划分，各个安全域之间限制严格的ACL，限制横向移动；
- 关闭不必要的共享权限以及端口，如：3389、445、135、139。
- 完善安全防护体系，保持良好的上网习惯，安全意识**是关键**。

▶▶ 2018年度最不安全密码报告

最烂密码

2018年末，密码管理公司SplashData公布了2018年度最新最烂密码，他们从500万个密码样本总结了这份榜单：

| | 2018 最不安全密碼名單前 25 名 | 跟 2017 比較 |
|--------|---------------------|-----------|
| 第 1 名 | 123456 | 不變 |
| 第 2 名 | password | 不變 |
| 第 3 名 | 123456789 | ↑3 |
| 第 4 名 | 12345678 | ↓1 |
| 第 5 名 | 12345 | 不變 |
| 第 6 名 | 111111 | 新入圍 |
| 第 7 名 | 1234567 | ↑1 |
| 第 8 名 | sunshine | 新入圍 |
| 第 9 名 | qwerty | ↓5 |
| 第 10 名 | <u>iloveyou</u> | 不變 |





弱口令调查

2017年11月，科技行业咨询企业EPC Group对600名用户进行调查，发现：

- 37%的受访者承认只有当网站要求他们更换密码时才会更改；
- 11%的受访者表示，同一个密码（或者稍有变化）至少会用7年；

数据泄露 – 如何应对?



- 发生重要泄漏事件后

□ 使用多个帐号密码体系:

- 一般网站群: 视频网站、游戏网站、各类论坛 等等...
- 重要帐号: 微信、支付宝、网银



▶▶ 数据泄露 – 如何应对?

□ 口令设置

找到一个生僻但易记的短语或句子（可以摘自歌曲、书本或电影），然后创建它的缩写形式，其中包括大写字母和标点符号等。

I like this DaShuaiGe!

My son Tom was born at
8:05

iLtDSG!

MsTwb@8:05

▶▶ 数据泄露 – 如何应对?

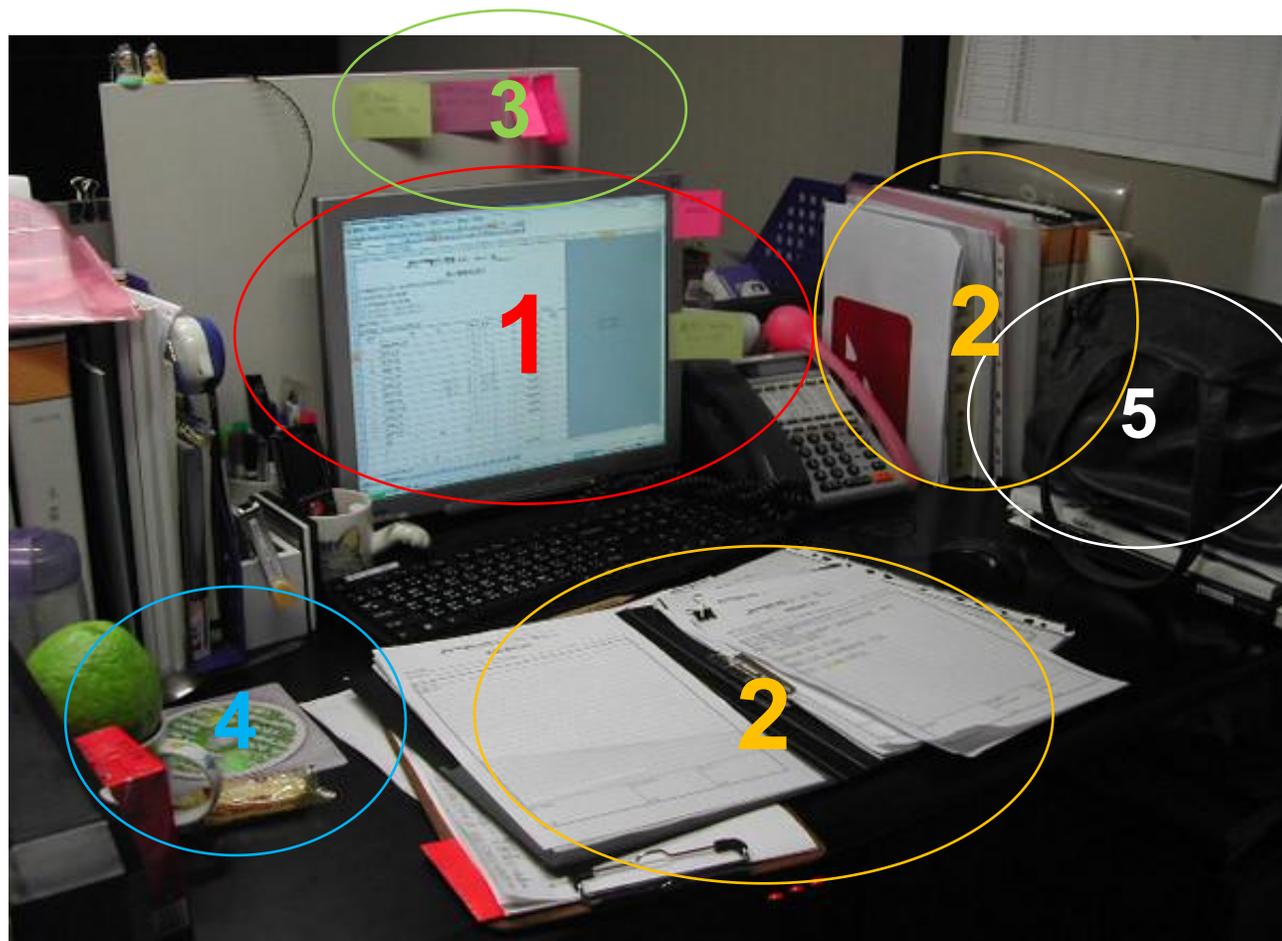
季军: FLZX3000cY4yhl9day
飞流直下三千尺, 疑似银河下九天

亚军: han-shansi.location()!∈[gusucity]
姑苏城外寒山寺

冠军: hold?fish:palm
鱼和熊掌不可兼得



问题出在哪里?



▶▶ 给普通员工的安全建议

□ 培养安全办公习惯

- 进入大门、闸机时主动阻止陌生人尾随进入；
- 陌生人员未经陪同出现在办公区域，应主动上前询问；
- 废弃的纸质资料应该进行充分粉碎（碎纸机）；
- 废弃的移动存储设备应交由IT部门消磁处理；
- 离开工位时对办公电脑进行锁屏；
- 敏感资料应妥善保管，在离开工位时锁入柜中；
- 不应使用来历不明的移动存储设备；
- 不应接入来历不明的WiFi热点；
-



环境安全



1. 不在网络或社交媒体上发布公司信息;
2. 不利用公司资源做非工作相关的信息交换;
3. 不在公共区域使用电话讨论公司机密信息;
4. 公司机密信息文件要妥善保存, 不带离办公区域;
5. 不在微信群中讨论公司机密信息。

弱口令、弱口令、弱口令!

某大型保险公司全网测试

- 网络架构、防护措施到位，无可利用的系统和应用漏洞；
- 发现边界存在一台JBoss主机，管理平台存在**弱口令**；
- 逐层渗透，控制大约200台服务器，最终成功获取**核心交易数据**。



| LRID | ACCOUNTID | ENTITYSID | BANKID | ACCOUNTAUTHCODE | ACCOUNTAUTHNUMBER | ACCOUNTAU | ENDDATE | SEGISD | ISACTV | CREATEDBY | CREATEDON | LASTMOOIFIED | | |
|-----------|------------|-----------|--------|---------------------|-------------------|-------------|---------|--------|--------|-----------|-----------|--------------|---------------------|------------|
| 112056072 | 2 | 6000001 | 1 | 621558111100291822 | 14815478 | 6215581111 | 918225 | 杨立岗 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056070 | 1322135003 | 6000001 | 1 | 622202111101542832 | 22172811 | 6222021111 | 428323 | 廖冬梅 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056067 | 1322135003 | 6000001 | 1 | 621226000100499501 | 15811594 | 6212260001 | 995011 | 黄平秋 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056066 | 1322135003 | 6000001 | 1 | 621558110500356953 | 15231791 | 6215581105 | 569524 | 蔡伟豪 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056065 | 1322135003 | 6000001 | 1 | 621226000102497349 | 13619812 | 6212260001 | 973494 | 黎煜辉 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056063 | 1322135003 | 6000001 | 1 | 621226110500086683 | 15581 | 6212261105 | 866810 | 万军 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056062 | 1322135003 | 6000001 | 1 | 622202110501353154 | 597136 | 6222021105 | 531542 | 张衡 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056060 | 1322135003 | 6000001 | 1 | 621558111100376059 | 32091453 | 6215581111 | 760590 | 廖金峰 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056058 | 1322135003 | 6000001 | 1 | 621288111100009278 | 28421092 | 6212881111 | 282787 | 江洪洪 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056057 | 1322135003 | 6000001 | 1 | 62220011110057774 | 28151103 | 6222001111 | 577749 | 潘树平 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056056 | 1322135003 | 6000001 | 1 | 622848040425127951 | 78239150 | 6228480404 | 279513 | 仇展展 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056055 | 1322135003 | 6000001 | 1 | 622208110500181872 | 13966212 | 6222081105 | 818726 | 许红霞 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056054 | 1322135003 | 6000001 | 1 | 622202110500398924 | 52021311 | 6222021105 | 989247 | 张耀林 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056053 | 1322135003 | 6000001 | 1 | 110502710130484016 | 51371152 | 1105027101 | 840166 | 张玉忠 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056052 | 2 | 6000001 | 1 | 622202111100478849 | 23702221 | 6222021111 | 788497 | 何春燕 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056051 | 2 | 6000001 | 1 | 622202111100211262 | 32784142 | 6222021111 | 212625 | 成碧美 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056049 | 2 | 6000001 | 1 | 622202111100364581 | 11523981 | 6222021111 | 645813 | 王武宇 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056048 | 2 | 6000001 | 1 | 622208111100061122 | 84831022 | 6222081111 | 811229 | 周朝斌 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056046 | 1322135003 | 6000001 | 1 | 622208111100408857 | 15815922 | 6222081111 | 288572 | 姜小燕 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056045 | 2 | 6000001 | 1 | 622208110500196868 | 34343121 | 6222081105 | 968687 | 廖福元 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056044 | 1322135003 | 6000001 | 1 | 622202111100402149 | 15811910 | 6222021111 | 221491 | 黄海珍 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056043 | 1322135003 | 6000001 | 1 | 1111134210110012818 | 11501180 | 11111342101 | 128188 | 王健 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056042 | 1322135003 | 6000001 | 1 | 955880110510402967 | 1521109 | 9558801105 | 296799 | 蔡洁 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056041 | 1322135003 | 6000001 | 1 | 622202110500605066 | 23317952 | 6222021105 | 506666 | 李伟翠 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |
| 112056040 | 2 | 6000001 | 1 | 622202111101005783 | 34831023 | 6222021111 | 257838 | 周朝斌 | (Null) | 6000001 | 1 | 2021030003 | 2014-11-04 09:25:44 | 2021030003 |

▶▶ 正确认识信息安全

“真正安全的计算机是拔下网线，断掉电源，放在地下掩体的保险柜中，并在掩体内充满毒气，在掩体外安排士兵守卫。”

-----绝对的安全是不存在的！

▶▶ 正确认识信息安全

“安全不只
态过程，它
系统工程，是



一次性的静
密结合的系
过程。”



信息安全人人有责



遵守单位的操作规程

设置强壮的密码，并定期修改



在系统建设、维护和使用中，基于本职工作，多考虑安全问题

做好终端安全配置，减少暴露的风险点



提高安全防范意识，多留心可疑事件，及时向本部门安全员报告