第三届
全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

集业界之力，共筑互联网安全

harite

腾讯安全应急响应中心（TSRC）负责人

对话·交流·合作

目录

- 安全之于腾讯
- 更多的挑战
- 应对的探索

安全之于腾讯

- 当谈到“安全”，对于腾讯意味着什么

  - **案例1：广告/诈骗消息**
  - **案例2：欺诈盗号**
  - **案例3：DDOS攻击**

安全之于腾讯

- 当谈到“安全”，对于腾讯意味着什么

  - **案例1：广告/诈骗消息**
  - **案例2：欺诈盗号**
  - **案例3：DDOS攻击**

安全之于腾讯

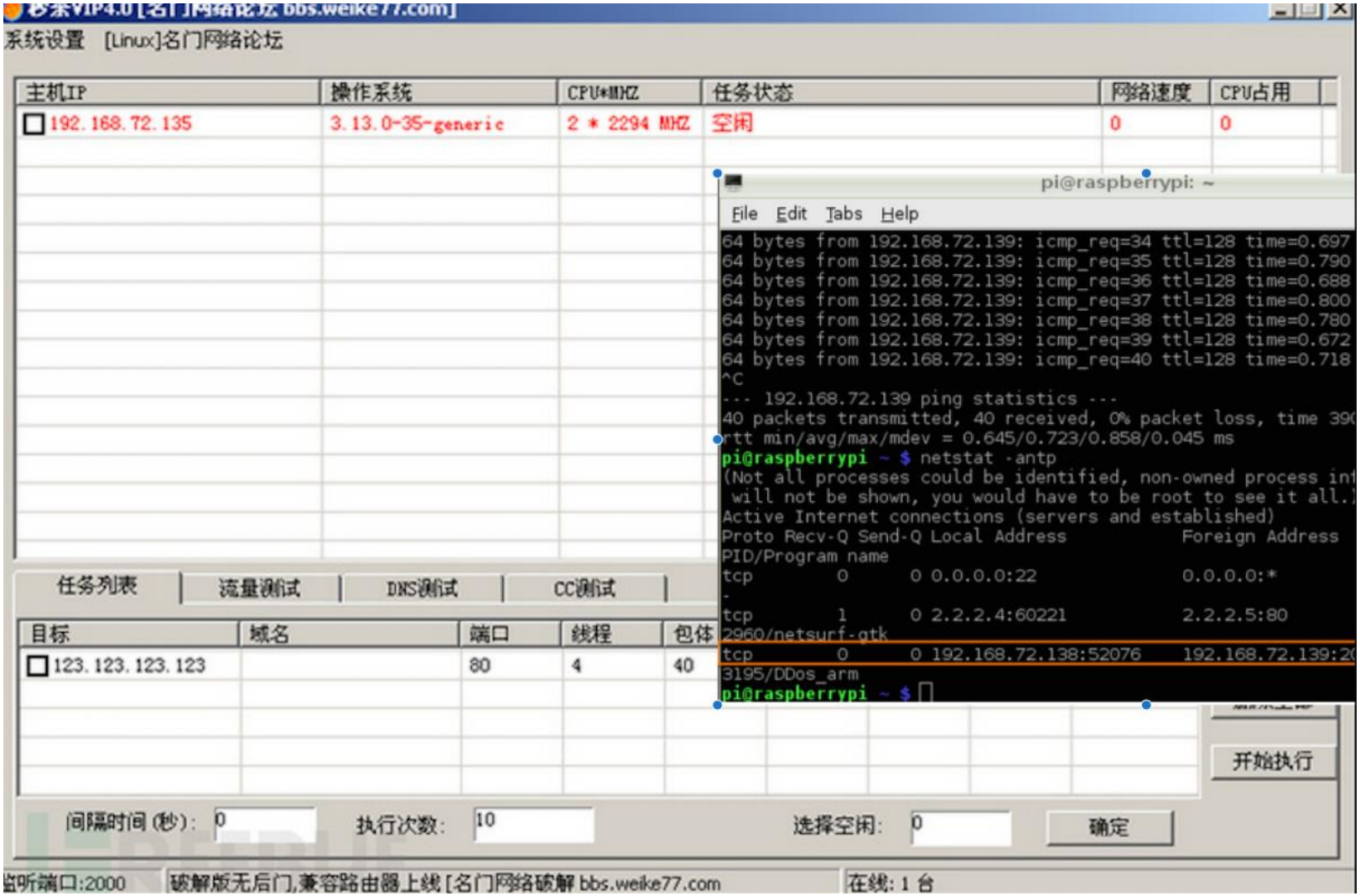
看小电影： 钓鱼攻击.avi

安全之于腾讯

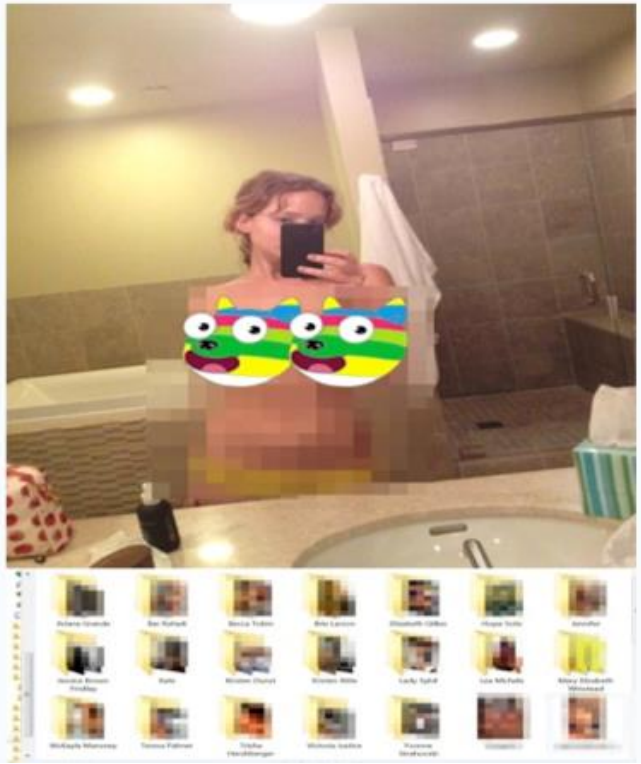
- 当谈到“安全”，对于腾讯意味着什么

  - **案例1：广告/诈骗消息**
  - **案例2：欺诈盗号**
  - **案例3：DDOS攻击**

更多的挑战


系统设置 [Linux]名门网络论坛
主机IP
操作系统
CPU*MHZ
任务状态
网络速度
CPU占用
192.168.72.135
3.13.0-35-generic
2 * 2294 MHZ
空闲
0
0
pi@raspberrypi: ~
File Edit Tabs Help
64 bytes from 192.168.72.139: icmp_req=34 ttl=128 time=0.697
64 bytes from 192.168.72.139: icmp_req=35 ttl=128 time=0.790
64 bytes from 192.168.72.139: icmp_req=36 ttl=128 time=0.688
64 bytes from 192.168.72.139: icmp_req=37 ttl=128 time=0.800
64 bytes from 192.168.72.139: icmp_req=38 ttl=128 time=0.780
64 bytes from 192.168.72.139: icmp_req=39 ttl=128 time=0.672
64 bytes from 192.168.72.139: icmp_req=40 ttl=128 time=0.718
^C
--- 192.168.72.139 ping statistics ---
40 packets transmitted, 40 received, 0% packet loss, time 39
rtt min/avg/max/mdev = 0.645/0.723/0.858/0.045 ms
pi@raspberrypi ~ $ netstat -antp
(Not all processes could be identified, non-owned process in
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address
PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:*
-
tcp 1 0 2.2.2.4:60221 2.2.2.5:80
2960/netsurf-gtk
tcp 0 0 192.168.72.138:52076 192.168.72.139:2
3195/DDos_arm
pi@raspberrypi ~ $
任务列表
流量测试
DNS测试
CC测试
目标
域名
端口
线程
包体
123.123.123.123
80
4
40
开始执行
间隔时间(秒):
0
执行次数:
10
选择空闲:
0
确定
监听端口:2000
破解版无后门,兼容路由器上线 [名门网络破解 bbs.weike77.com
在线: 1 台

更多的挑战



China-based online “Password Recovery” services:
You pay them to hack into “your” account.

300 Yuan ($43) to break an overseas mailbox password, with 85% probability of success.

200 Yuan ($29) to break a domestic mailbox password, with 90% probability of success.

1000 Yuan ($143) to break a company’s mailbox password (no success rate given).

Also on the menu:
passwords for 163, 126, QQ, Yahoo, Sohu, Sina, TOM, Hotmail, MSN…etc.

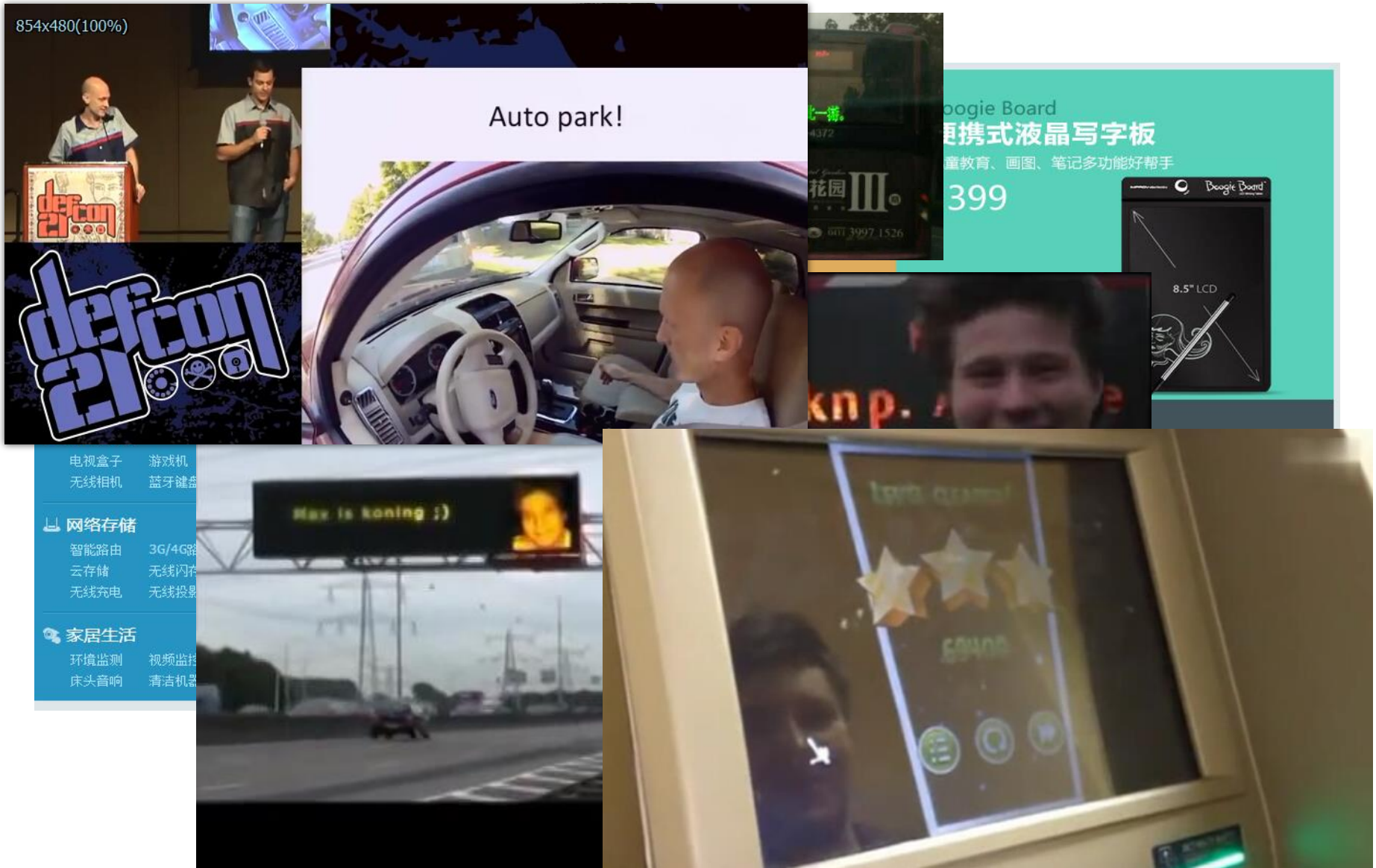
Mailbox passwords for sale, Chinese hacker business or scam?
http://www.thedarkvisitor.com/2008/04/mailbox-passwords-for-sale-chinese-hacker-business-or-scam/
http://news.cnnb.com.cn/system/2008/04/14/005548483.shtml

更多的挑战

HeartBlee


```
@@ -643,8 +645,8 @@ OSStatus FindSigAlg(SSLContext *ctx,
643 645         }
644 646
645 647 fail:
```

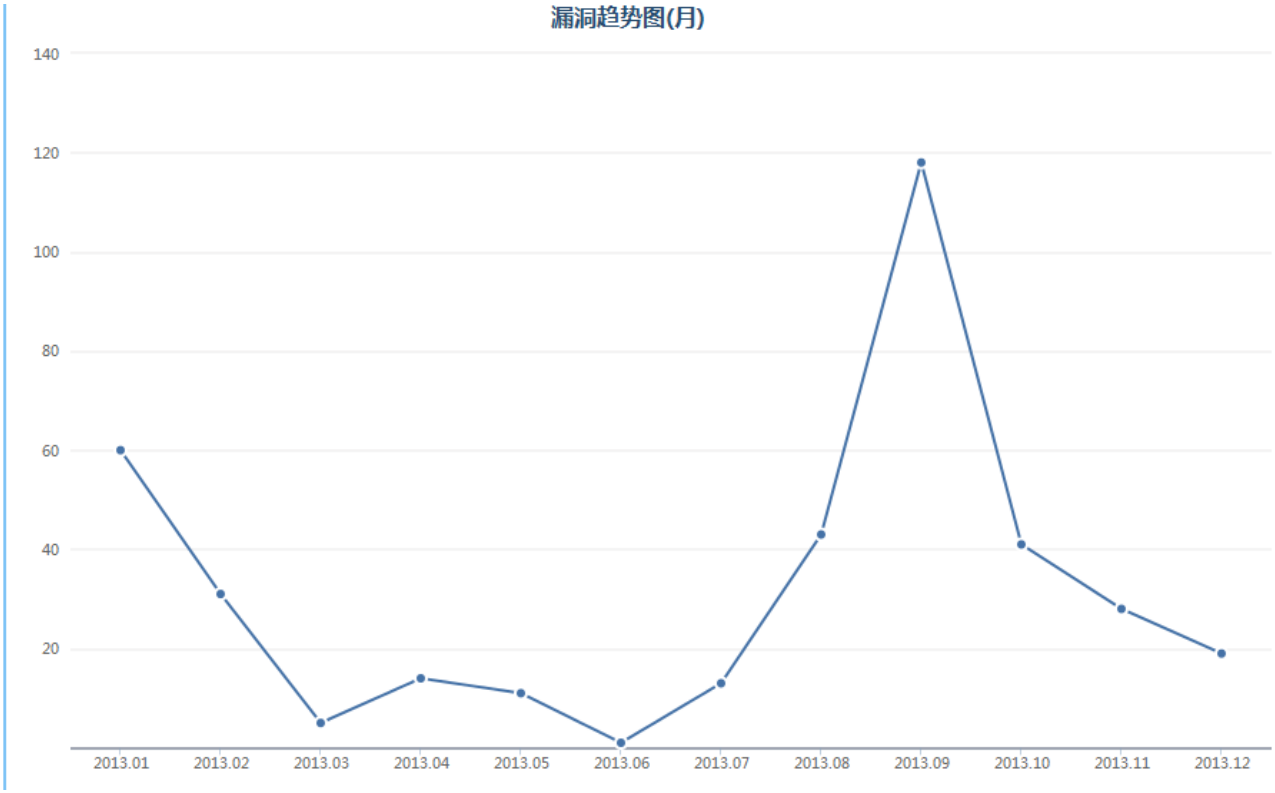
更多的挑战


854x480(100%)
Auto park!
Boogie Board
便携式液晶写字板
399
8.5" LCD
电视盒子
游戏机
无线相机
网络存储
智能路由
云存储
无线充电
家居生活
环境监测
床头音响

应对的探索

500人+ / 6000+vuls / 350万+

应对的探索



自有安全系统的正向促进

应对的探索

为了更好地保障互联网用户安全，腾讯安全应急响应中心（TSRC）专门制定了"通用软件漏洞奖励计划"，以现金方式奖励和收集白帽子发现的通用软件漏洞并遵循负责任的安全漏洞披露过程予以处理。

【适用条件】

1、影响腾讯及其他厂商的广泛使用的通用软件，优先以下列表：
操作系统：Linux 、iOS 、Android
应用软件：PHP、Apache、OpenSSL、nginx、Tomcat、struts、JAVA
2、漏洞危害级别为严重或高（一般是远程可以利用且危害较大），具体评估标准见后文；
3、漏洞未在外部公开，且需要提供可用的PoC；
4、通过腾讯"安全漏洞反馈平台"提交，类目选择"通用软件"

【评分标准】

注意：根据漏洞影响，还会提供**1~50**万不等的额外现金奖励

危害等级	漏洞危害	示例	分值范围
严重	远程获取服务器权限	直接的远程任意代码执行。 如溢出、命令注入	9~10

把控IT基础设施的风险

应对的探索

信息共享&合作

应对的探索

- 敏感数据保护
- 移动终端安全
- 无线安全
- 智能设备安全
- IT基础软件安全研究

欢迎合作