小电台

Weifeng Sun

School of Software, DLUT

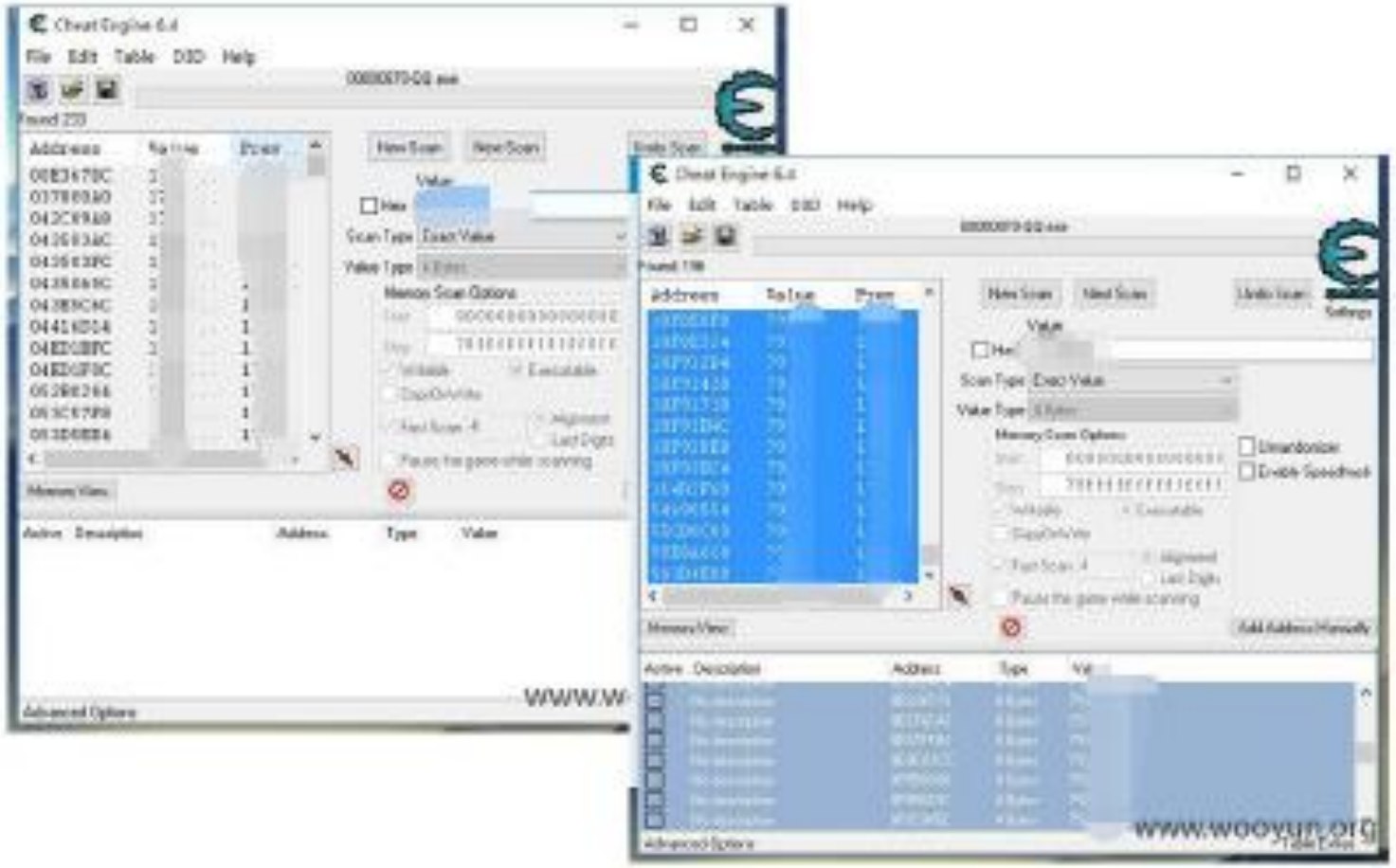
11月11日

- 传文件要加密！QQ的离线文件功能将点对点传输升级为云存储下载，极大的改变了文件传输体验。但该技术是将你传的文件保存在云端，那当你不在线的时候这些文件是否还安全呢？他人是否可以看到你曾经传给别人的内容？腾讯QQ存漏洞可下载任意用户离线传输过的文件

漏洞作者：路人甲	相关厂商：腾讯
事件编号：WooYun-2015-143395	

QQ的离线文件功能将文件传输“点对点”升级为“云存储”，令用户明显的感觉到了云计算对各种使用场景的改善。但云存储是将文保存在云服务器上，那当您不在线的时候这些数据是否还安全呢？

很多用户都因游戏作弊目的，对“内存修改”这一神技了如指掌。乌云的一位白帽子，却用内存修改法，发现了QQ离线文件功能存在的一处惊人漏洞，他竟然能够看到和下载任意用户有效期内的离线文件！



首先登录一个自己的QQ，然后随便选用一款内存搜索/修改功能于一体的软件，白帽子的是Cheat Engine（这名字，明明是游戏作弊的嚒）在内存中搜索自己的QQ号码，改成你想看的任意用户QQ号。

接下来，就是见证奇迹的时刻！打开你本地QQ的“我的共享”功能，没错，这就是离线文件存储的地方，你会发现，你竟然看到了对方曾经的离线传输文件内容！！

接下来，就是见证奇迹的时刻！打开你本地QQ的“我的共享”功能，没错，这就是离线文件存储的地方，你会发现，你竟然看到了对方曾经的离线传输文件内容！！

3月5日

- 微信红包

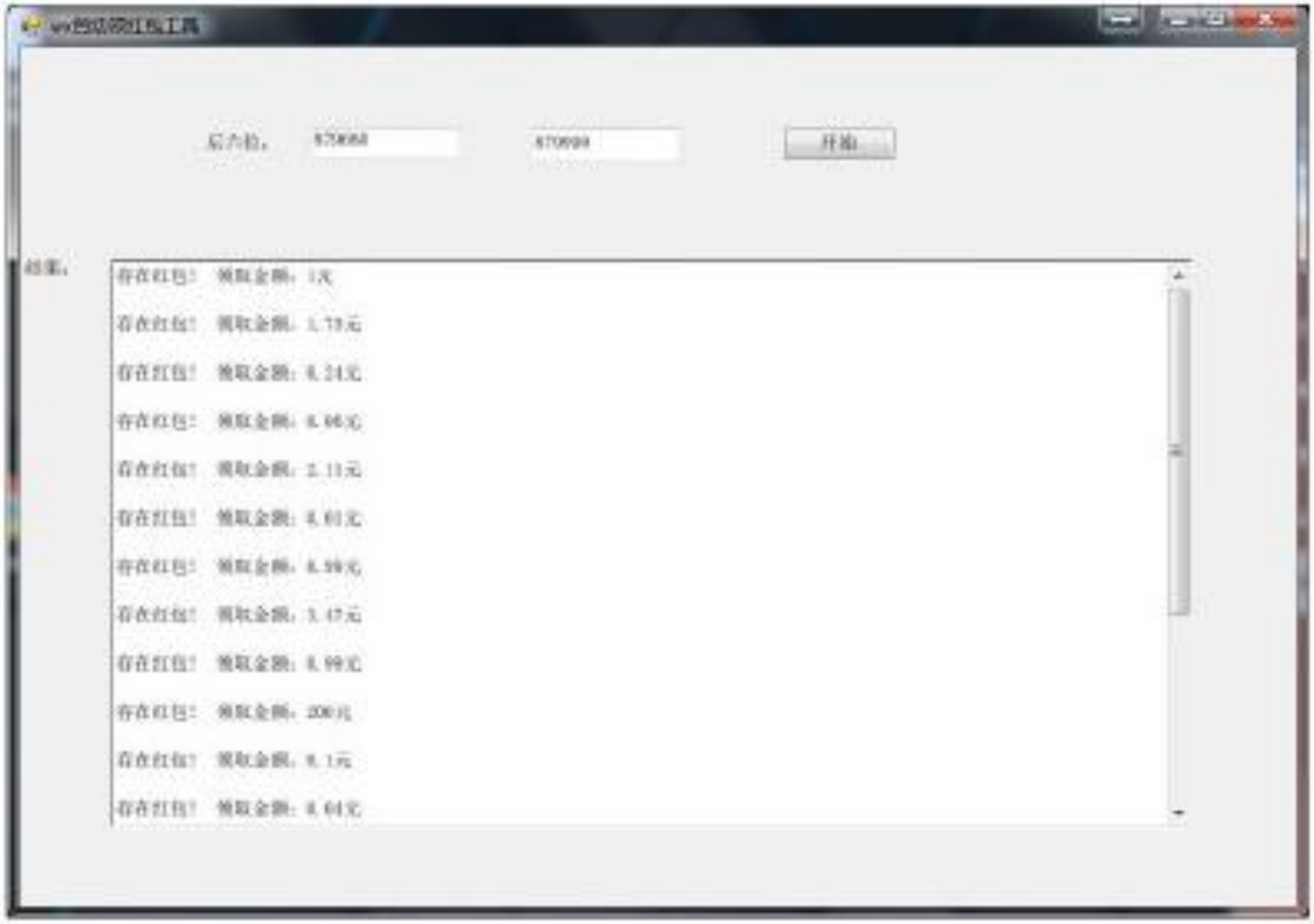
- 可越权抢到其他用户发的红包，不到二十分钟就能进账200

漏洞编号：WooYun-2015-90898

如果曾经你给朋友包的红包被陌生人领走了，那很可能是遭遇到了类似的红包任意领取的漏洞。。。

通过分析得到红包地址，有个叫“sendid”的，就是红包的id。只要修改这个id后面的几位数字，就能打开其他任意用户的红包，比如这几个包白帽子也不知道是谁

用程序实现自动挂机领红包，一觉醒来发现已经发家致富奔小康也是不无可能的，天天躺着就把钱给挣了（因过于暴利，请网友切勿模仿）



挂机前

挂机（不到20分钟）

最后给大家讲个惊悚故事——网络金融。。。

知名杀软Avast被关键字屏蔽

- http://www.williamlong.info/archives/4160.html **2015-3-2 19:14:59**
- Avast被屏蔽的方式是关键字屏蔽，被屏蔽的关键字是“.avast.com”，大家可以尝试访问 http://www.microsoft.com/?.avast.com 来进行测试。
- Avast被封锁域名应该是人为操作屏蔽的，估计和其提供的SecureLine VPN服务有关，Avast提供的这个服务可以“加密网络连接，防范间谍，使用安全线防护您的隐私。”

Google无人机今年实现首飞，从天空带来互联网服务

- http://www.leiphone.com/news/201503/0Vyaeo2OQQMM9rdv.html 2015-03-03
- Titan团队
- 目前全球大约有四十亿人无法连接互联网，Pichai希望利用无人机来改善这一现状。
  - WMN？
  - 兴趣组报名

D-Link（友讯）路由器存在远程命令注入漏洞

- http://www.freebuf.com/news/59861.html 2015-03-03
- 首先是D-Link DIR636L型号的路由器对“ping”工具上的输入信息过滤不当导致攻击者可以在路由器上注入任意命令；其次是认证机制在执行过程中也出现了错误，所以攻击者可以远程获得设备的root权限。既然攻击者可以修改路由器上的防火墙或者NAT规则，那么他就可对其他网络发动DDoS攻击或者直接把连接路由器的计算机暴露于公网。
- 基于ping.ccp漏洞的属性，用户只要访问嵌入恶意HTTP form的网页，攻击者就可获得设备的root访问权限，劫持DNS设置或者在受害者设备上执行任意命令。

- Wormhole
- Onion network
  - 兴趣组选题

DNS下载数据

- 如何在渗透测试中利用BASH和DNS下载数据
  - 在渗透测试过程中，防火墙一般都会禁止服务器对外建立连接，这种情况下使用DNS来下载数据是一种行之有效的方法。
  - http://www.freebuf.com/articles/system/57183.html
  - 兴趣组选题
  - 2015-01-2

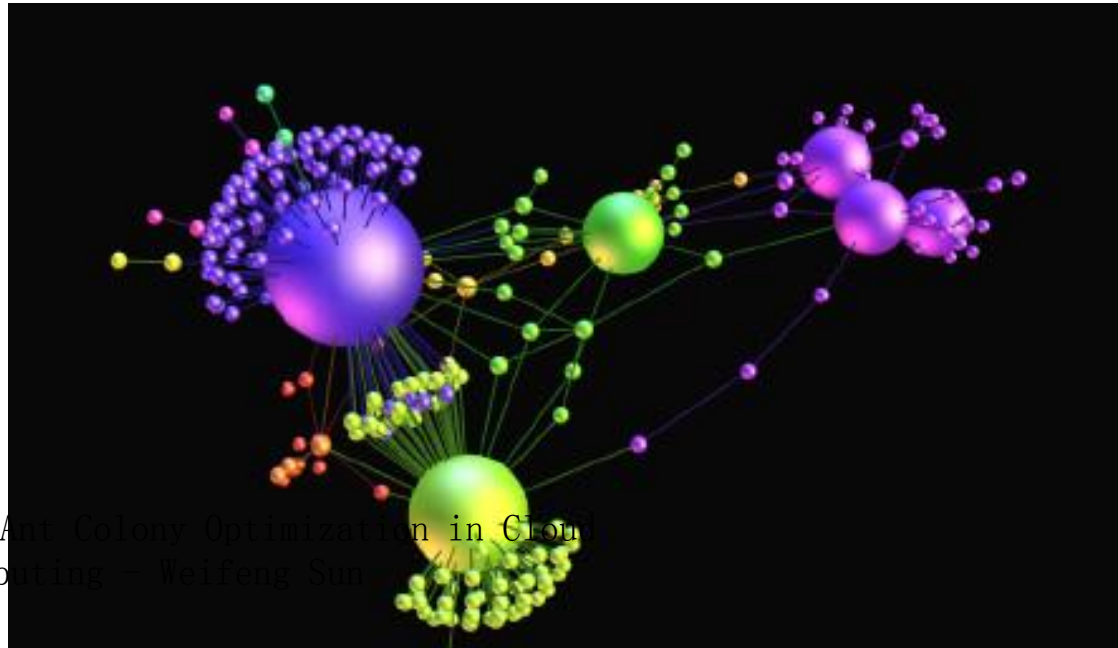
朝鲜互联网全面宕机 疑遭美国攻击

- 2014-12-23
- 美国互联网基础设施监测公司Dyn Research称，周一朝鲜互联网全面宕机，具体原因不明，分析专家表示可能由于路由软件问题或遭受网络攻击。美国总统奥巴马上周五郑重许诺，称将对索尼影业遭到的黑客攻击事件作出回应，并将此次事件归咎于朝鲜。（朝鲜有互联网吗？

- 朝鲜通过中国联通发布4条/8路由，这是它目前接入互联网的方式（还有卫星公司intelsat的备份链路）我们确实看到22号23号有针对朝鲜的几个ip的比较大的ddos攻击。最近的一次打的是朝鲜的某基础设施，攻击类型udp ssdp放大攻击，早上9点刚攻击结束

DNS和bot

- dns ddos的一些bot连接dns server的图，看的出来有的bot是配置的连接多个dns server（图中大球）来发动攻击的
- 兴趣组选题



- ICMP 重定向
- http://www.potaroo.net/presentations/2014-02-27-dnssec.pdf

- 之前不能用是因为windows, linux默认都不支持icmp重定向。但新的andrioid, mac osx都默认支持icmp重定向。其实比这个技术厉害的是ipv6 RA, 通杀。
- IPv6 RA 兴趣组选题

- 非技术类

机票改签骗局再现 十几分钟三次转账一万八没了

- 大连新闻网 2015-11-12 13:58
- http://toutiao.com/i6216146717549527553/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android

央视315揭秘背后:家庭WiFi存在更大隐患

- http://mp.weixin.qq.com/s?__biz=MjM5ODAwMzgyMA==&mid=203933418&idx=3&sn=6943c1d12de4d2846549c0c4dc67bfbd
- 3月15日央视一套315晚会现场上演了一场令人印象深刻的真人秀，由专业网络安全工程师充当的黑客伪装了晚会演播室的免费WiFi，500余名观众当场自拍，并在不知不觉中通过黑客的WiFi热点在朋友圈发照片。不可思议的是，现场观众刚刚拍摄的照片和手机绑定的邮箱密码居然全部出现在了舞台后方的大屏幕上。

新加坡政府官网遭黑客入侵发布李光耀逝世假消息2015-03-19

- http://toutiao.com/a4096118137/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android

哈尔滨公交IC卡被破解了

- 黑龙江电视台 2015-10-31
- 仨男子在超市爆刷4万元被发现丨交待说下个软件就破了
- http://toutiao.com/i6211671789861847554/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android
- 啥软件？谁有兴趣查一查

中国家用WiFi常见密码TOP10

- I
- h
3
ig
m
u

常见密码 TOP 10

排名	密码	数量	占比	累计占比
1	12345678	3048	3.256%	3.256%
2	123456789	2460	2.628%	5.885%
3	88888888	1453	1.552%	7.437%
4	1234567890	711	0.760%	8.197%
5	00000000	406	0.434%	8.631%
6	87654321	351	0.375%	9.006%
7	66668888	335	0.358%	9.363%
8	11223344	316	0.338%	9.701%
9	147258369	313	0.334%	10.035%
10	11111111	299	0.319%	10.355%

美官方称“中国黑客窃取一切” 打算对华使用制裁语言

- http://tthz.huanqiu.com/viewTouTiao.html?newId=6709767&f=jrtt&tt_from=mobile_qq&tt_group_id=6189252133593825538

Android再爆新漏洞 国产手机全中招

- http://toutiao.com/a5259911148/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android
- Certifi-gate
- mSRTs
- 兴趣组选题

奇迹：英国男子给国际空间站打电话，成功通话50秒

- 08-07
- http://toutiao.com/i5235410524/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android

彩票官员改开奖程序中8878万

- 新浪体育 2015-07-2
- http://toutiao.com/i4822290333/?tt_from=mobile_qq&utm_campaign=client_share&app=news_article&utm_source=mobile_qq&iid=3235617795&utm_medium=toutiao_android

周三交作业

- 电子版
- 二选一
  - 兴趣组选题、打算。留联系方式
  - Wooyun漏洞总结（分析），500字以上，不超过3个


もぐもぐ
うまうま
72時間以内に新しくメロンを2つ用意しろ.

Q&A

- Thank you!

- Weifeng Sun孙伟峰 wfsun@dlut.edu.cn
- **Associate Professor**
- **School of Software,DLUT**